SAN-Konfigurationshandbuch (für iSCSI)

ESX 4.1

ESXi 4.1

vCenter Server 4.1

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter http://www.vmware.com/de/support/pubs.

DE-000288-00

vmware®

Die neueste technische Dokumentation finden Sie auf der VMware-Website unter:

http://www.vmware.com/de/support/pubs/

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

Copyright © 2009, 2010 VMware, Inc. Alle Rechte vorbehalten. Dieses Produkt ist durch Urheberrechtsgesetze, internationale Verträge und mindestens eines der unter http://www.vmware.com/go/patents-de aufgeführten Patente geschützt.

VMware ist eine eingetragene Marke oder Marke der VMware, Inc. in den USA und/oder anderen Ländern. Alle anderen in diesem Dokument erwähnten Bezeichnungen und Namen sind unter Umständen markenrechtlich geschützt.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

Über dieses Handbuch 5

1 Verwenden von ESX/ESXi mit einem iSCSI-SAN (Storage Area Network) 7
- Grundlegendes zu Virtualisierung 7
- iSCSI-SAN-Konzepte 9
- Übersicht über die Verwendung von ESX/ESXi in einem SAN 14
- Besonderheiten bei der Verwendung von SAN-Speicher mit ESX/ESXi 16
- Grundlegendes VMFS-Datenspeicher 17
- Entscheidungen zur Verwendung von LUNs 18
- Zugriff auf Daten in einem SAN durch virtuelle Maschinen 21
- Grundlegendes zu Multipathing und Failover 21
- Auswählen von Speicherorten für virtuelle Maschinen 27
- Vorbereitung auf einen Serverausfall 28
- LUN-Anzeige und erneutes Prüfen 29

2 Konfigurieren von iSCSI-Initiatoren und -Speicher 31
- Anforderungen an ESX/ESXi-iSCSI-SAN 32
- Beschränkungen für ESX/ESXi-iSCSI-SAN 32
- Festlegen der LUN-Zuordnungen 32
- Netzwerkkonfiguration und Authentifizierung 33
- Einrichten von unabhängigen Hardware-iSCSI-Adaptern 33
- Einrichten und Konfigurieren von abhängigen Hardware-iSCSI-Adaptern 35
- Einrichten und Konfigurieren des Software-iSCSI-Adapters 37
- Netzwerkkonfiguration für Software-iSCSI und abhängige Hardware-iSCSI 39
- Binden von iSCSI-Ports an iSCSI-Adapter 43
- Verwenden von Jumbo-Frames mit iSCSI 45
- Aktivieren von Jumbo-Frames für Software-iSCSI und abhängige Hardware-iSCSI 45
- Konfigurieren von Erkennungsadressen für iSCSI-Initiatoren 46
- Konfigurieren von CHAP-Parametern für iSCSI-Adapter 48
- Konfigurieren zusätzlicher Parameter für iSCSI 52
- iSCSI-Sitzungsverwaltung 54
- Hinzufügen von iSCSI-Speicher 56

3 Ändern von SAN-Speichersystemen für ESX/ESXi 59
- Testen der ESX/ESXi-SAN-Konfigurationen 59
- Allgemeine Überlegungen zu iSCSI-SAN-Speichersystemen 60
- EMC CLARiiON-Speichersysteme 60
- EMC Symmetrix-Speichersysteme 61
- Aktivieren von HP StorageWorks MSA1510i für die Kommunikation mit ESX/ESXi 62
- HP StorageWorks EVA-Speichersysteme 63
- NetApp-Speichersysteme 63

EqualLogic-Speichersysteme 66
LeftHand Networks SAN/iQ-Speichersysteme 66
Dell PowerVault MD3000i-Speichersysteme 67
iSCSI-Ziele in vApps 67

4 Starten von einem iSCSI-SAN 69
Allgemeine Empfehlungen für das Starten von einem iSCSI-SAN 70
Vorbereiten des iSCSI-SAN 70
Konfigurieren von ESX-Hosts für das Starten über ein iSCSI-SAN 71
iBFT-iSCSI-Start - Überblick 72
Erfassen von Diagnoseinformationen für ESXi-Hosts 77

5 Verwalten von ESX/ESXi-Systemen, die einen SAN-Speicher verwenden 79
Anzeigen von Informationen zu Speicheradaptern 79
Anzeigen von Informationen zu Speichergeräten 80
Anzeigen von Datenspeicherinformationen 83
Beheben von Problemen bei der Speicheranzeige 84
Prüfen und Beanspruchen von Pfaden 89
Gemeinsame Nutzung von Diagnosepartitionen 94
Vermeiden und Beheben von SAN-Problemen 95
Optimieren der SAN-Speicherleistung 95
Beheben von Leistungsproblemen 99
Überlegungen zu SAN-Speichersicherungen 103
Verwalten von duplizierten VMFS-Datenspeichern 105
Speicherhardware-Beschleunigung 108

A iSCSI SAN-Konfiguration - Checkliste 111

B VMware vSphere-Befehlszeilenschnittstelle 113
resxtop-Befehl 113
vicfg-iscsi-Befehl 113
vicfg-mpath-Befehl 113
esxcli corestorage claimrule-Befehl 114
vmkping-Befehl 114

C Verwalten von Multipathing-Modulen und Hardwarebeschleunigungs-Plug-Ins 115
Verwalten von Speicherpfaden und Multipathing-Plug-Ins 115
Verwalten des Hardwarebeschleunigungsfilters und der Hardwarebeschleunigungs-Plug-Ins 122
esxcli corestorage claimrule - Optionen 125

Index 127

Über dieses Handbuch

Im *SAN-Konfigurationshandbuch (für iSCSI)* wird die Verwendung der VMware® ESX™- und VMware ESXi-Systeme mit einem iSCSI-SAN (Storage Area Network) erläutert. Das Handbuch schließt begriffliche Hintergrundinformationen sowie die Installationsanforderungen für ESX, ESXi und VMware vCenter™ Server ein.

Zielgruppe

Die Informationen in diesem Handbuch sind für erfahrene Systemadministratoren bestimmt, die mit der Windows- oder Linux-VM-Technologie und Datencenteroperationen vertraut sind.

VMware Technical Publications - Glossar

VMware Technical Publications stellt einen Glossar mit Begriffen zur Verfügung, die Ihnen möglicherweise nicht vertraut sind. Definitionen von Begriffen wie sie in der technischen Dokumentation von VMware genutzt werden finden Sie unter http://www.vmware.com/support/pubs.

Feedback zu diesem Dokument

VMware freut sich über Ihre Vorschläge zum Verbessern der Dokumentation. Falls Sie Anmerkungen haben, senden Sie diese bitte an: docfeedback@vmware.com.

VMware vSphere-Dokumentation

Die Dokumentation zu VMware vSphere umfasst die kombinierte Dokumentation zu VMware vCenter Server und ESX/ESXi.

Technischer Support und Schulungsressourcen

Ihnen stehen die folgenden Ressourcen für die technische Unterstützung zur Verfügung. Die aktuelle Version dieses Handbuchs sowie weiterer Handbücher finden Sie auf folgender Webseite: http://www.vmware.com/support/pubs.

Online- und Telefon-Support Auf der folgenden Webseite können Sie über den Onlinesupport technische Unterstützung anfordern, Ihre Produkt- und Vertragsdaten abrufen und Produkte registrieren: http://www.vmware.com/support.

Kunden mit entsprechenden Support-Verträgen erhalten über den telefonischen Support schnelle Hilfe bei Problemen der Prioritätsstufe 1. Rufen Sie die folgende Webseite auf: http://www.vmware.com/support/phone_support.html.

Support-Angebote

Informationen dazu, wie die Support-Angebote von VMware Sie dabei unterstützen, Ihre geschäftlichen Anforderungen zu erfüllen, finden Sie auf der folgenden Webseite: http://www.vmware.com/support/services.

VMware Professional Services

Die VMware Education Services-Kurse umfassen umfangreiche Praxisübungen, Fallbeispiele und Kursmaterialien, die zur Verwendung als Referenztools bei der praktischen Arbeit vorgesehen sind. Kurse können vor Ort, im Unterrichtsraum und live online durchgeführt werden. Für Pilotprogramme vor Ort und die Best Practices für die Implementierung verfügt VMware Consulting Services über Angebote, die Sie bei der Beurteilung, Planung, Erstellung und Verwaltung Ihrer virtuellen Umgebung unterstützen. Informationen zu Schulungen, Zertifizierungsprogrammen und Consulting-Diensten finden Sie auf der folgenden Webseite: http://www.vmware.com/services.

Verwenden von ESX/ESXi mit einem iSCSI-SAN (Storage Area Network) 1

Sie können ESX/ESXi in Verbindung mit einem SAN (Storage Area Network) verwenden, ein spezielles Hochgeschwindigkeitsnetzwerk, das Computersysteme mit Hochleistungsspeicher-Subsystemen verbindet. Der Einsatz von ESX/ESXi zusammen mit einem SAN bietet zusätzlichen Speicher für Konsolidierungen, steigert die Zuverlässigkeit und unterstützt Sie bei der Notfallwiederherstellung.

Die effiziente Nutzung von ESX/ESXi mit einem SAN setzt voraus, dass Sie über Anwendungserfahrungen mit ESX/ESXi-Systemen und SAN-Konzepten verfügen. Darüber hinaus ist es erforderlich, bei der Einrichtung von ESX/ESXi-Hosts für die Verwendung von iSCSI (Internet SCSI)-SAN-Speichersystemen bestimmte Überlegungen anzustellen.

Dieses Kapitel behandelt die folgenden Themen:

- „Grundlegendes zu Virtualisierung“, auf Seite 7
- „iSCSI-SAN-Konzepte“, auf Seite 9
- „Übersicht über die Verwendung von ESX/ESXi in einem SAN“, auf Seite 14
- „Besonderheiten bei der Verwendung von SAN-Speicher mit ESX/ESXi“, auf Seite 16
- „Grundlegendes VMFS-Datenspeicher“, auf Seite 17
- „Entscheidungen zur Verwendung von LUNs“, auf Seite 18
- „Zugriff auf Daten in einem SAN durch virtuelle Maschinen“, auf Seite 21
- „Grundlegendes zu Multipathing und Failover“, auf Seite 21
- „Auswählen von Speicherorten für virtuelle Maschinen“, auf Seite 27
- „Vorbereitung auf einen Serverausfall“, auf Seite 28
- „LUN-Anzeige und erneutes Prüfen“, auf Seite 29

Grundlegendes zu Virtualisierung

Sowohl VMware-Desktopprodukte (wie VMware Workstation) als auch VMware-Serverprodukte (wie VMware ESX/ESXi) verfügen im Allgemeinen über die VMware-Virtualisierungsebene. Diese Ebene bietet eine konsistente Plattform für Entwicklung, Tests, Bereitstellung und Support von Anwendungsarbeitslasten.

Die Virtualisierungsebene ist wie folgt strukturiert:

- Jede virtuelle Maschine führt ein eigenes Betriebssystem (das Gastbetriebssystem) und eigene Anwendungen aus.
- Die Virtualisierungsebene ermöglicht die Zuweisung virtueller Geräte zu Anteilen bestimmter physischer Geräte. Zu diesen Geräten zählen die virtualisierte CPU, Arbeitsspeicher, E/A-Busse, Netzwerkschnittstellen, Speicheradapter und -geräte, Eingabegeräte für Benutzer und das BIOS.

Netzwerkvirtualisierung

Die Virtualisierungsebene gewährleistet, dass jede virtuelle Maschine von anderen virtuellen Maschinen isoliert ist. Virtuelle Maschinen können ausschließlich über Netzwerkmechanismen miteinander kommunizieren, die ähnlich denen zur Verbindung separater physischer Maschinen sind.

Die Isolierung ermöglicht Administratoren, interne Firewalls oder andere Netzwerkisolierungsumgebungen einzurichten, über die einige virtuelle Maschinen mit externen Geräten verbunden werden können, während andere ausschließlich über virtuelle Netzwerke mit anderen virtuellen Maschinen verbunden sind.

Speichervirtualisierung

ESX/ESXi bietet eine Speichervirtualisierung auf Hostebene, die die physische Speicherebene von virtuellen Maschinen logisch abstrahiert.

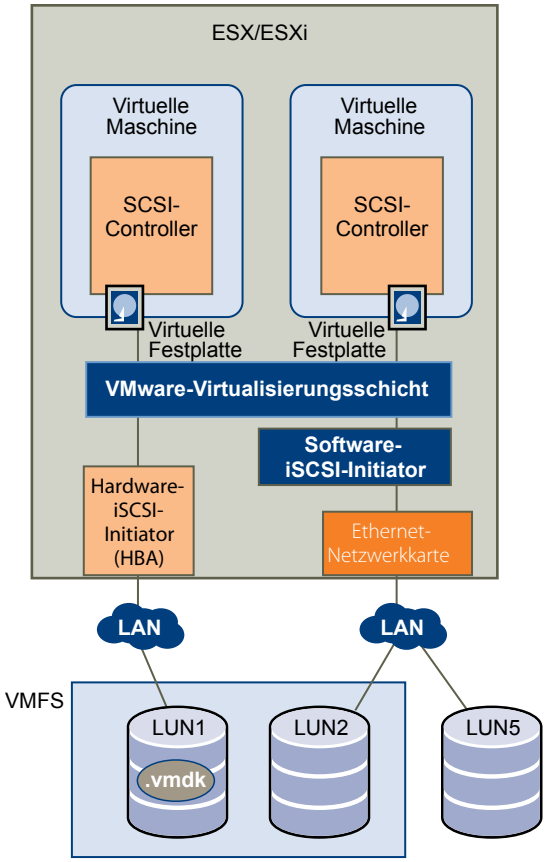
Eine virtuelle Maschine in ESX/ESXi verwendet eine virtuelle Festplatte, um das Betriebssystem, die Programmdateien und andere Daten für ihren Betrieb zu speichern. Eine virtuelle Festplatte ist eine große physische Datei bzw. Zusammenstellung von Dateien, die sich so einfach wie jede andere Datei kopieren, verschieben, archivieren und sichern lässt. Sie können virtuelle Maschinen mit mehreren virtuellen Festplatten konfigurieren.

Für den Zugriff auf virtuelle Festplatten verwendet eine virtuelle Maschine virtuelle SCSI-Controller. Zu diesen virtuellen Controllern gehören BusLogic Parallel, LSI Logic Parallel, LSI Logic SAS und VMware Paravirtual. Diese Controller sind die einzigen SCSI-Controllertypen, die eine virtuelle Maschine anzeigen und auf die sie zugreifen kann.

Jede virtuelle Festplatte, auf die eine virtuelle Maschine über einen der virtuellen SCSI-Controller zugreifen kann, befindet sich auf einem VMware VMFS-Datenspeicher, auf einem NFS-basierten Datenspeicher oder auf einer Raw-Festplatte. Jede virtuelle Festplatte wird vom Standpunkt der virtuellen Maschine aus so angezeigt, als wäre ein SCSI-Laufwerk mit einem SCSI-Controller verbunden. Ob auf das tatsächliche physische Festplattengerät über parallele SCSI-, iSCSI-, Netzwerk- oder Fibre-Channel-Adapter auf dem Host zugegriffen wird, wird auf dem Gastbetriebssystem und den Anwendungen, die auf der virtuellen Maschine ausgeführt werden, angezeigt.

Abbildung 1-1 bietet eine Übersicht über die Speichervirtualisierung. Das Diagramm stellt den Speicher dar, der VMFS einsetzt, sowie den Speicher, der die Raw-Gerätezuordnung einsetzt, verwendet. Das Diagramm zeigt auch, wie der Zugriff auf iSCSI-Speicher entweder durch iSCSI-HBAs oder über eine Mehrzweck-Netzwerkkarte erfolgt, die eine iSCSI-Initiator-Software nutzt.

Abbildung 1-1. Die iSCSI-SAN-Speichervirtualisierung



iSCSI-SAN-Konzepte

Wenn Sie ein ESX/ESXi-Administrator sind, der ESX/ESXi-Hosts zusammen mit SANs einsetzen möchte, müssen Sie über Anwendungserfahrungen mit SAN-Konzepten verfügen. Weitere Informationen zur SAN-Technologie finden Sie in Printmedien oder dem Internet.

iSCSI-SANs verwenden Ethernet-Verbindungen zwischen Computersystemen oder Hostservern und Hochleistungsspeichersystemen. Zu den SAN-Komponenten zählen iSCSI-Hostbusadapter (HBAs) oder Netzwerkkarten in den Hostservern, Switches und Routern, die Speicherdatenverkehr weiterleiten, in der Verkabelung, in den Speicherprozessoren (SP) und in den Festplattenspeichersystemen.

iSCSI-SAN verwendet eine Client-Server-Architektur. Der Client, der so genannte iSCSI-Initiator, ist auf Ihrem Host in Betrieb. Er initiiert iSCSI-Sitzungen, indem er SCSI-Befehle ausgibt und diese in das iSCSI-Protokoll eingekapselt an den Server überträgt. Der Server ist als iSCSI-Ziel bekannt. Dieses iSCSI-Ziel stellt ein physisches Speichersystem auf dem Netzwerk dar. Es kann auch von einem virtuellen iSCSI-SAN bereitgestellt werden, z. B. einem in einer virtuellen Maschine ausgeführten iSCSI-Zielemulator. Das iSCSI-Ziel reagiert auf die Befehle des Initiators, indem es die erforderlichen iSCSI-Daten überträgt.

Ports im iSCSI-SAN

Ein einzelnes erkennbares Element auf dem iSCSI-SAN, z. B. ein Initiator oder ein Ziel, stellt einen iSCSI-Knoten dar. Jeder Knoten besitzt mindestens einen Port, der mit dem SAN verbunden wird.

iSCSI-Ports sind Endpunkte einer iSCSI-Sitzung. Jeder Knoten kann auf mehrere Arten ermittelt werden.

IP-Adresse Jeder iSCSI-Knoten kann über eigene IP-Adresse verfügen, sodass Router und Switches im Netzwerk eine Verbindung zwischen dem Server und dem Speicher aufbauen können. Diese Adresse ist mit der IP-Adresse vergleichbar, die Sie Ihrem Computer zuweisen, um auf das Unternehmensnetzwerk oder das Internet zugreifen zu können.

iSCSI-Name Ein weltweit eindeutiger Name zum Identifizieren des Knotens. iSCSI verwendet die Formate IQN (iSCSI Qualified Name), EUI (Extended Unique Identifier) und NAA (Network Address Authority).

iSCSI-Namen für Ihre iSCSI-Initiatoren werden in der Regel auf einen eindeutigen Standardwert gesetzt, zum Beispiel `iqn.1998–01.com.vmware:iscsites–tox–68158ef2`. Der Standardwert muss daher nicht geändert werden. Wenn Sie ihn dennoch ändern, stellen Sie sicher, dasss der neue iSCSI-Name eindeutig ist.

iSCSI-Alias Ein Name für ein iSCSI-Gerät oder einen iSCSI-Port, der einfach zu verwalten ist und statt dem iSCSI-Namen verwendet wird. iSCSI-Aliase sind nicht eindeutig und sollen als benutzerfreundliche Namen dienen, die mit einem Port verknüpft werden können.

iSCSI-Benennungskonventionen

iSCSI verwendet einen speziellen, eindeutigen Bezeichner zum Identifizieren eines iSCSI-Knotens, sei es ein Ziel oder ein Initiator. Dieser Name entspricht dem WWN (WorldWide Name), der mit Fibre-Channel-Geräten verknüpft ist und zur allgemeinen Knotenidentifikation dient.

iSCSI-Namen können zwei verschiedene Formate aufweisen. Das geläufigste Format ist IQN.

Weitere Informationen zu Benennungskonventionen und Zeichenfolgenprofilen finden Sie unter RFC 3721, RFC 3722 und RFC 3980 auf der IETF-Website.

Das IQN-Format (iSCSI Qualified Name)

IQN hat das Format `iqn.jjjj–mm.Namensvergabestelle:eindeutiger Name`, wobei:

- *yyyy-mm* gibt Jahr und Monat an, in dem die Stelle für die Namensvergabe (Naming Authority) eingerichtet wurde.
- *Namensvergabestelle* ist üblicherweise die Syntax des Internetdomänennames der Namensvergabestelle in umgekehrter Reihenfolge. Zum Beispiel könnte die Namensvergabestelle iscsi.vmware.com den qualifizierten iSCSI-Namen „iqn.1998-01.com.vmware.iscsi“ haben. Der Name gibt an, dass der Domänenname vmware.com im Januar 1998 registriert wurde und es sich bei „iscsi“ um eine Unterdomäne von vmware.com handelt.
- *eindeutiger_Name* steht für einen beliebigen Namen, z. B. den Namen des Hosts. Die Namensvergabestelle muss sicherstellen, dass alle zugewiesenen Namen nach dem Doppelpunkt eindeutig sind, z. B.:
  - iqn.1998-01.com.vmware.iscsi:Name1
  - iqn.1998-01.com.vmware.iscsi:Name2
  - iqn.1998-01.com.vmware.iscsi:Name999

Das EUI-Format (Enterprise Unique Identifier)

EUI hat das Format `eui.`*`16 hexadezimale Ziffern`*.

Beispiel: `eui.0123456789ABCDEF`.

Bei den 16 Hexadezimalstellen handelt es sich um die Textdarstellung einer 64-Bit-Zahl eines IEEE-EUI-Schemas (Extended Unique Identifier). Die oberen 24 Bit identifizieren die Unternehmens-ID, die das IEEE einem bestimmten Unternehmen zuordnet. Die unteren 40 Bit werden durch die Entität zugewiesen, der diese Unternehmens-ID zugeordnet ist, und müssen eindeutig sein.

iSCSI-Initiatoren

Für den Zugriff auf iSCSI-Ziele verwendet Ihr Host iSCSI-Initiatoren. Die Initiatoren übertragen SCSI-Anforderungen und Antworten, die in das iSCSI-Protokoll eingekapselt sind, zwischen dem Host und dem iSCSI-Ziel.

VMware unterstützt verschiedene Initiatortypen.

Software iSCSI-Adapter

Ein Software-iSCSI-Adapter ist ein im VMkernel integrierter VMware-Code. Er ermöglicht die Verbindung Ihres Hosts mit dem iSCSI-Speichergerät über Standardnetzwerkadapter. Der Software iSCSI-Adapter dient der iSCSI-Verarbeitung und kommuniziert gleichzeitig mit dem Netzwerkadapter. Mit dem Software iSCSI-Adapter können Sie die iSCSI-Technologie verwenden, ohne besondere Hardware erwerben zu müssen.

Hardware iSCSI-Adapter

Bei einem Hardware-iSCSI-Adapter handelt es sich um einen Adapter eines Drittanbieters, der die gesamte iSCSI- und Netzwerkverarbeitung von Ihrem Host auslagert. Hardware-iSCSI-Adapter werden in Kategorien unterteilt.

Abhängige Hardware-iSCSI-Adapter

Hängt vom VMware-Netzwerk sowie von den iSCSI-Konfigurations- und -Verwaltungsschnittstellen ab, die von VMware zur Verfügung gestellt werden.

Bei diesem Adaptertyp kann es sich um eine Karte handeln, die einen Standard-Netzwerkadapter und die iSCSI-Offload-Funktion für denselben Port bietet. Die iSCSI-Offload-Funktion ist hinsichtlich des Abrufens der IP- und der MAC-Adresse sowie anderer Parameter für iSCSI-Sitzungen von der Netzwerkkonfiguration des Hosts abhängig. Ein Beispiel für einen abhängigen Adapter ist die iSCSI-lizenzierte Broadcom 5709-Netzwerkkarte.

Unabhängige Hardware-iSCSI-Adapter

Implementiert ein eigenes Netzwerk und eigene iSCSI-Konfigurations- und -Verwaltungsschnittstellen.

Ein Beispiel für einen unabhängigen Hardware-iSCSI-Adapter ist eine Karte, die entweder nur die iSCSI-Offload-Funktion oder die iSCSI-Offload-Funktion und die standardmäßige Netzwerkkarten-Funktion bietet. Die iSCSI-Offload-Funktion besitzt eine unabhängige Konfigurationsverwaltung, die die IP- und die MAC-Adresse sowie andere Parameter für die iSCSI-Sitzungen zuweist. Ein Beispiel für einen unabhängigen Adapter ist der QLogic QLA4052-Adapter.

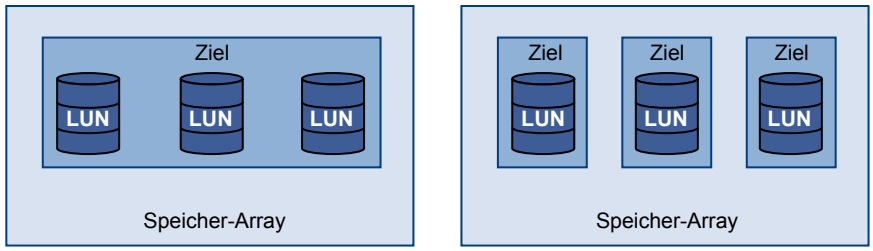
Hardware-iSCSI-Adapter müssen möglicherweise lizenziert werden. Anderenfalls werden sie nicht im vSphere Client oder im vSphere-CLI angezeigt. Fragen Sie Ihren Anbieter nach Lizenzierungsinformationen.

Ziel im Vergleich zu LUN-Darstellungen

Im ESX/ESXi-Kontext beschreibt der Begriff „Ziel“ eine einzelne Speichereinheit, auf die Ihr Host zugreifen kann. Die Begriffe „Speichergerät“ und „LUN“ beschreiben ein logisches Volume, das Speicherplatz auf einem Ziel darstellt. In der Regel stehen die Begriffe „Gerät“ und „LUN“ im ESX/ESXi-Kontext für ein SCSI-Volume, das Ihrem Host von einem Speicherziel angeboten wird und formatiert werden kann

Verschiedene iSCSI-Speicheranbieter verwenden unterschiedliche Methoden, um Speicher für Server bereitzustellen. Einige Anbieter stellen mehrere LUNs auf einem einzigen Ziel dar, während andere Anbieter mehrere Ziele mit je einer LUN verknüpfen. Wenngleich die Speichernutzung durch einen ESX/ESXi-Host ähnlich ist, ist dennoch die Darstellungsweise der Informationen durch Verwaltungsprogramme unterschiedlich.

Abbildung 1-2. Ziel im Vergleich zu LUN-Darstellungen



Im vorliegenden Beispiel sind in jeder dieser Konfigurationen drei LUNs verfügbar. Im ersten Fall erkennt ESX/ESXi ein Ziel, obwohl in diesem Ziel drei LUNs vorhanden sind, die verwendet werden können. Jede LUN steht für ein einzelnes Speichervolume. Im zweiten Fall werden dem ESX/ESXi-Host drei unterschiedliche Ziele mit je einer LUN angezeigt.

ESX/ESXi-basierte iSCSI-Initiatoren richten nur eine Verbindung zu jedem Ziel ein. Das bedeutet, dass sich der LUN-Datenverkehr bei Speichersystemen mit einem Ziel, das mehrere LUNs umfasst, auf diese eine Verbindung konzentriert. Sind in einem System drei Ziele mit je einer LUN vorhanden, bestehen drei Verbindungen zwischen einem Host und den drei verfügbaren LUNs. Diese Information ist hilfreich, um den Speicherdatenverkehr auf mehreren Verbindungen des ESX/ESXi-Hosts mit mehreren iSCSI-HBAs zusammenzufassen, wobei der Datenverkehr für ein Ziel auf einen bestimmten HBA festgelegt und gleichzeitig für den Datenverkehr zu einem anderen Ziel ein anderer HBA genutzt werden kann.

Multipathing und Pfad-Failover

Bei der Datenübertragung zwischen dem Hostserver und dem Speicher nutzt das SAN eine Technik, die als Multipathing bezeichnet wird. Multipathing bietet die Möglichkeit, mehr als einen physischen Pfad vom ESX/ESXi-Host zu einer LUN in einem Speichersystem bereitzustellen.

In der Regel besteht ein einzelner Pfad von einem Host zu einer LUN aus einem iSCSI-Adapter oder der Netzwerkkarte, Switch-Ports, Verbindungskabeln und dem Speicher-Controller-Port. Falls eine Komponente des Pfads ausfällt, wählt der Host für E/A-Vorgänge einen anderen verfügbaren Pfad. Der Prozess der Erkennung eines ausgefallenen Pfads und des Wechsels auf einen anderen Pfad wird als Pfad-Failover bezeichnet.

Speichersystemtypen

ESX/ESXi unterstützt verschiedene Speichersysteme und Arrays.

Zu den Speichertypen, die Ihr Host unterstützt, gehören Aktiv-Aktiv, Aktiv-Passiv und ALUA-konform.

Aktiv-Aktiv-Speichersystem Ermöglicht den gleichzeitigen Zugriff auf die LUNs über alle Speicherports, die ohne wesentlichen Leistungsabfall verfügbar sind. Alle Pfade sind jederzeit aktiv (es sei denn, ein Pfad fällt aus).

Aktiv-Passiv-Speichersystem Ein System, in dem ein Speicherprozessor aktiv den Zugriff auf eine vorhandene LUN ermöglicht. Die anderen Prozessoren fungieren als Sicherung für die LUN und können den Zugriff auf andere LUN-E/A-Vorgänge aktiv bereitstellen. E/A-Daten können ausschließlich an einen aktiven Port gesendet werden. Falls der Zugriff über den aktiven Speicherport fehlschlägt, kann einer der passiven Speicherprozessoren durch die Server, die auf ihn zugreifen, aktiviert werden.

Asymmetrisches Speichersystem Unterstützt Asymmetric Logical Unit Access (ALUA). ALUA-konforme Speichersysteme bieten verschiedene Zugriffsebenen für einzelne Ports. ALUA ermöglicht es Hosts, den Status von Zielports festzustellen und Pfade zu priorisieren. Der Host verwendet einige der aktiven Pfade als primäre Pfade, andere als sekundäre Pfade.

Speichersystem mit virtuellem Port Ermöglicht den Zugriff auf alle verfügbaren LUNs über einen einzigen virtuellen Port. Dies sind Aktiv/Aktiv-Speichergeräte, die jedoch die Vielzahl der Verbindungen durch einen einzigen Port verdecken. Für das ESX/ESXi-Multipathing ist nicht erkennbar, dass es sich dabei um mehrere Verbindungen zum Speicher handelt. Port-Failover und der Verbindungsausgleich werden von diesen Speichersystemen transparent verarbeitet. Dieser Vorgang wird häufig als „transparentes Failover“ bezeichnet.

Erkennung, Authentifizierung und Zugriffssteuerung

Sie können mehrere Mechanismen verwenden, um Ihren Speicher zu erkennen und den Zugriff darauf zu beschränken.

Damit die Richtlinie für die Speicherzugriffssteuerung unterstützt wird, müssen Sie den Host und das iSCSI-Speichersystem konfigurieren.

Erkennung

Eine Erkennungssitzung ist Teil des iSCSI-Protokolls und gibt die auf einem iSCSI-Speichersystem verfügbaren Ziele zurück. ESX/ESXi bietet zwei verschiedene Erkennungsmethoden: dynamisch und statisch. Bei der dynamischen Erkennung wird eine Liste der verfügbaren Ziele aus dem iSCSI-Speichersystem abgerufen, wohingegen Sie bei der statischen Erkennung lediglich versuchen können, über den Zielnamen auf ein bestimmtes Ziel zuzugreifen.

Authentifizierung

Die Authentifizierung durch iSCSI-Speichersysteme erfolgt nach Name und Schlüsselpaar. ESX/ESXi unterstützt das CHAP-Protokoll, das für die SAN-Implementierung empfohlen wird. Sowohl für den ESX/ESXi-Host als auch für das iSCSI-Speichersystem muss das CHAP-Protokoll aktiviert sein und beide müssen die gleichen Anmeldeinformationen verwenden, um die CHAP-Authentifizierung verwenden zu können.

Zugriffssteuerung

Zugriffssteuerung ist eine auf dem iSCSI-Speichersystem eingerichtete Richtlinie. Eine Vielzahl der Implementierungen unterstützen mindestens eine der drei folgenden Arten der Zugriffssteuerung:

- Nach Initiatorname
- Nach IP-Adresse
- Nach dem CHAP-Protokoll

Nur Initiatoren, die alle Richtlinien einhalten, können auf das iSCSI-Volume zugreifen.

Fehlerkorrektur

Um die Integrität von iSCSI-Headern und -Daten zu schützen, legt das iSCSI-Protokoll Methoden zur Fehlerkorrektur fest, die als Header- und Daten-Digests bezeichnet werden.

Beide Parameter sind standardmäßig deaktiviert, können aber von Benutzern aktiviert werden. Diese Digests beziehen sich auf den Header bzw. die SCSI-Daten, die zwischen iSCSI-Initiatoren und Zielen in beiden Richtungen übertragen werden.

Header- und Daten-Digests überprüfen die durchgängige Integrität unverschlüsselter Daten. Diese Prüfung geht über die Integritätsprüfungen hinaus, die andere Netzwerkebenen bereitstellen (z.B. TCP und Ethernet). Header- und Daten-Digests prüfen den gesamten Kommunikationspfad mit allen Elementen, die den Datenverkehr auf Netzwerkebene ändern können, wie Router, Switches und Proxys.

Die Bereitstellung und Art dieser Digests wird verhandelt, sobald eine iSCSI-Verbindung aufgebaut wird. Wenn der Initiator und das Ziel einer Digest-Konfiguration zustimmen, muss dieses Digest für den gesamten Datenverkehr zwischen diesem Initiator und dem Ziel verwendet werden.

Die Aktivierung von Header- und Daten-Digests erfordert eine zusätzliche Verarbeitung durch den Initiator und das Ziel, was zu einer Beeinträchtigung des Durchsatzes und der CPU-Leistung führen kann.

HINWEIS Systeme, die Intel Nehalem-Prozessoren einsetzen, lagern die iSCSI Digest-Berechnungen aus und reduzieren damit die Auswirkungen auf die Leistung.

Übersicht über die Verwendung von ESX/ESXi in einem SAN

Die Verwendung von ESX/ESXi in einem SAN erhöht die Flexibilität, Effizienz und Zuverlässigkeit. Bei der Verwendung von ESX/ESXi mit einem SAN werden eine zentrale Verwaltung sowie Failover- und Lastausgleichstechnologien ebenfalls unterstützt.

Im Folgenden werden die Vorteile der Verwendung von ESX/ESXi mit einem SAN zusammengefasst:

- Sie haben die Möglichkeit, Daten sicher zu speichern und mehrere Pfade zu Ihrem Speicher zu konfigurieren, um solch eine Fehlerquelle auszuschließen.
- Die Fehlerresistenz wird durch die Verwendung eines SAN mit ESX/ESXi-Systemen auf die Server erweitert. Wenn Sie einen SAN-Speicher einsetzen, können alle Anwendungen nach einem Ausfall des ursprünglichen Hosts umgehend auf einem anderen Host neu gestartet werden.
- Mit VMware VMotion können Sie während des laufenden Systembetriebs Migrationen virtueller Maschinen durchführen.
- Verwenden Sie VMware High Availability (HA) zusammen mit einem SAN, um die virtuellen Maschinen mit ihrem zuletzt bekannten Status auf einem anderen Server neu zu starten, falls ihr Host ausfällt.
- Verwenden Sie VMware Fault Tolerance (FT), um geschützte virtuelle Maschinen auf zwei unterschiedlichen Hosts zu replizieren. Die virtuellen Maschinen werden weiterhin unterbrechungsfrei auf dem sekundären Host ausgeführt, falls der primäre Host ausfällt.

- Verwenden Sie VMware DRS (Distributed Resource Scheduler), um virtuelle Maschinen für den Lastausgleich von einem Host auf einen anderen Host zu migrieren. Da sich der Speicher in einem freigegebenen SAN-Array befindet, werden Anwendungen ohne Unterbrechung weiter ausgeführt.
- Wenn Sie VMware DRS-Cluster verwenden, versetzten Sie einen ESX/ESXi-Host in den Wartungsmodus, um alle ausgeführten virtuellen Maschinen auf andere ESX/ESXi-Hosts zu migrieren. Anschließend können Sie auf dem ursprünglichen Host Upgrades oder andere Wartungsvorgänge durchführen.

Die Portabilität und Kapselung von virtuellen VMware-Maschinen ergänzt die Eigenschaften des Speichers hinsichtlich der gemeinsamen Nutzung. Wenn sich virtuelle Maschinen in einem SAN-basierten Speicher befinden, können Sie eine virtuelle Maschine auf einem Server herunterfahren und diese auf einem anderen Server starten oder diese auf einem Server anhalten und den Betrieb auf einem anderen Server im selben Netzwerk wieder aufnehmen – und das in nur wenigen Minuten. Auf diese Weise können Sie Rechenressourcen migrieren und gleichzeitig einen konsistenten gemeinsamen Zugriff aufrechterhalten.

Anwendungsbeispiele für ESX/ESXi und SAN

Bei Verwendung von ESX/ESXi mit einem SAN können Sie eine Reihe von Aufgaben ausführen.

Die Verwendung von ESX/ESXi in Verbindung mit einem SAN ist für die folgenden Aufgaben hilfreich:

Wartung ohne Ausfallzeiten

Bei der Wartung von ESX/ESXi-Hosts oder -Infrastrukturen sollten Sie VMware DRS oder VMotion für die Migration virtueller Maschinen auf andere Server verwenden. Falls im SAN ein gemeinsamer Speicher vorhanden ist, kann die Wartung für Benutzer virtueller Maschinen ohne Unterbrechungen durchgeführt werden.

Lastausgleich

Verwenden Sie VMotion oder VMware DRS, um virtuelle Maschinen für einen Lastausgleich auf andere Hosts zu migrieren. Falls in einem SAN ein gemeinsamer Speicher vorhanden ist, kann der Lastausgleich für Benutzer virtueller Maschinen ohne Unterbrechungen durchgeführt werden.

Speicherkonsolidierung und Vereinfachung des Speicherlayouts

Wenn Sie mit mehreren Hosts arbeiten und auf jedem Host mehrere virtuelle Maschinen ausgeführt werden, reicht der Speicher des Hosts nicht mehr aus und es wird externer Speicher benötigt. Die Wahl eines SAN für die externe Datenspeicherung führt zu einer einfacheren Systemarchitektur und bietet gleichzeitig andere Vorteile.

Beginnen Sie mit der Reservierung eines großen Volumes und ordnen Sie anschließend Teile nach Bedarf virtuellen Maschinen zu. Die Volume-Zuordnung und Erstellung aus dem Speichergerät müssen nur einmal durchgeführt werden.

Notfallwiederherstellung

Das Speichern sämtlicher Daten in einem SAN kann die Remotespeicherung von Datensicherungen erheblich vereinfachen. Zudem können Sie virtuelle Maschinen zur Wiederherstellung auf ESX-Remotehosts neu starten, falls die Wiederherstellung am ursprünglichen Standort nicht möglich ist.

Vereinfachte Array-Migrationen und Speicher-Upgrades

Wenn Sie neue Speichersysteme oder -Arrays erwerben, verwenden Sie Storage VMotion, um eine automatisierte Migration der Festplattendateien virtueller Maschinen vom vorhandenen Speicher zum neuen Speicherziel ohne Unterbrechungen für die Benutzer virtueller Maschinen durchzuführen.

Suche nach weiteren Informationen

Zusätzlich zu diesem Dokument stehen eine Vielzahl weiterer Hilfsmittel zur Verfügung, die Sie bei der Konfiguration des ESX/ESXi-Systems in einem SAN nutzen können.

- Weitere Informationen zur Installation finden Sie in der Dokumentation Ihres Speicher-Array-Anbieters. Der Speicher-Array-Anbieter kann Ihnen möglicherweise ebenfalls Dokumentationen zur Verwendung des Speichersystems in einer ESX/ESXi-Umgebung bereitstellen.
- Die VMware-Dokumentations-Website.
- Das *SAN-Konfigurationshandbuch (für Fibre-Channel)* erläutert die Verwendung von ESX/ESXi in einem Fibre-Channel-SAN.
- Das *Handbuch zur E/A-Kompatibilität für VMware* enthält eine Liste der aktuell genehmigten HBAs, HBA-Treiber und Treiberversionen.
- Das *Speicher-/SAN-Kompatibilitätshandbuch* von VMware enthält eine Liste der aktuell genehmigten Speicher-Arrays.
- Die *VMware-Versionshinweise* stellen Informationen zu bekannten Problemen und Umgehungen bereit.
- Die *VMware-Knowledgebase* bietet Informationen zu allgemeinen Problemen und Umgehungen.

Besonderheiten bei der Verwendung von SAN-Speicher mit ESX/ESXi

Die Verwendung eines SANs in Verbindung mit einem ESX/ESXi-Host unterscheidet sich von der herkömmlichen SAN-Verwendung in vielerlei Hinsicht.

Beachten Sie bei der Verwendung von SAN-Speicher mit ESX/ESXi folgende Punkte:

- Ein direkter Zugriff auf das Betriebssystem der virtuellen Maschine, das den Speicher verwendet, ist nicht möglich. Mit herkömmlichen Tools können Sie ausschließlich das VMware ESX/ESXi-Betriebssystem überwachen. Über den vSphere-Client können Sie virtuelle Maschinen überwachen.
- Der für die SAN-Verwaltungstools sichtbare HBA gehört zum ESX/ESXi-System und nicht zum Teil der virtuellen Maschine.
- Das ESX/ESXi-System führt für Sie ein Multipathing durch.

Verwaltungsanwendungen von Drittanbietern

Sie können Verwaltungssoftware von Drittanbietern in Verbindung mit Ihrem ESX/ESXi-Host verwenden.

Häufig ist im Lieferumfang der iSCSI-Speicherhardware eine Speicherverwaltungssoftware enthalten. Hierbei handelt es sich in der Regel um eine Webanwendung, die mit einem beliebigen Webbrowser ausgeführt werden kann, der mit dem Netzwerk verbunden ist. In anderen Fällen wird die Software typischerweise auf dem Speichersystem oder einem Einzelserver ausgeführt, der unabhängig von den Servern betrieben wird, die das SAN zum Speichern nutzen.

Verwenden Sie diese Verwaltungssoftware von Drittanbietern für die folgenden Aufgaben:

- Speicher-Array-Verwaltung, einschließlich LUN-Erstellung, Cacheverwaltung des Arrays, LUN-Zuordnung und LUN-Sicherheit.
- Einrichtung von Replikations-, Prüfpunkt-, Snapshot- bzw. Spiegelungsfunktionen.

Wenn Sie die SAN-Verwaltungssoftware auf einer virtuellen Maschine verwenden, können Sie die Vorteile der Ausführung einer virtuellen Maschine nutzen, einschließlich Failover mit VMotion, Failover mit VMware HA. Aufgrund der zusätzlichen Indirektionsebene ist das SAN jedoch für die Verwaltungssoftware möglicherweise nicht sichtbar. In diesem Fall können Sie eine RDM verwenden.

HINWEIS Die erfolgreiche Ausführung der Verwaltungssoftware durch eine virtuelle Maschine hängt letztlich von dem betreffenden Speichersystem ab.

Grundlegendes VMFS-Datenspeicher

Zum Speichern virtueller Festplattendateien verwendet ESX/ESXi Datenspeicher. Datenspeicher sind logische Container, bei denen Angaben zu den einzelnen Speichergeräten verborgen bleiben und die ein einheitliches Modell für die Speicherung der Dateien virtueller Maschinen bieten. Auf Speichergeräten bereitgestellte Datenspeicher verwenden in der Regel das VMFS (VMware Virtual Machine File System)-Format, ein spezielles Hochleistungsdateisystem für die Speicherung virtueller Maschinen.

Ein VMFS-Datenspeicher kann mehrere virtuelle Maschinen ausführen. Darüber hinaus bietet VMFS eine verteilte Dateisperrung für virtuelle Maschinen, sodass die virtuellen Maschinen sicher in einer SAN-Umgebung betrieben werden können, in der mehrere ESX/ESXi-Hosts denselben VMFS-Datenspeicher gemeinsam nutzen.

Mit dem vSphere-Client können Sie im Voraus einen VMFS-Datenspeicher auf einem blockbasierten Speichergerät einrichten, das Ihr ESX/ESXi-Host erkennt. Ein VMFS-Datenspeicher kann sich über mehrere physische Erweiterungsgeräte erstrecken, einschließlich SAN-LUNs und lokale Speicher. Diese Funktion ermöglicht Ihnen die Zusammenfassung von Speicher und gibt Ihnen bei der Erstellung des für die virtuelle Maschine erforderlichen Datenspeichers die notwendige Flexibilität.

Die Kapazität des Datenspeichers kann während der Ausführung von virtuellen Maschinen im Datenspeicher erhöht werden. Auf diese Weise lässt sich entsprechend den aktuellen Anforderungen der virtuellen Maschine stets neuer Speicherplatz zu VMFS-Volumes hinzufügen. VMFS wurde für den gleichzeitigen Zugriff mehrerer physischer Maschinen konzipiert und erzwingt eine geeignete Zugriffsteuerung für VM-Dateien.

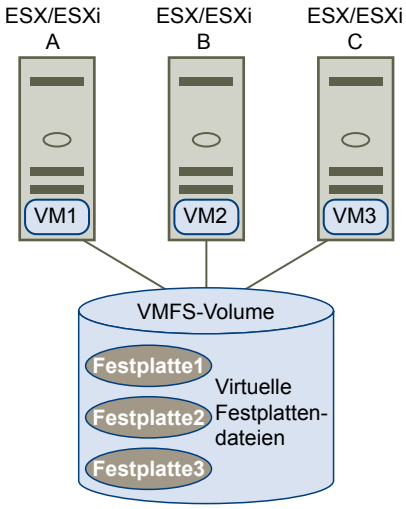
Gemeinsame Verwendung eines VMFS-Datenspeichers auf mehreren ESX/ESXi-Hosts

Als Clusterdateisystem ermöglicht VMFS mehreren ESX/ESXi-Hosts, parallel auf denselben VMFS-Datenspeicher zuzugreifen.

Um zu gewährleisten, dass nicht mehrere Server gleichzeitig auf dieselbe virtuelle Maschine zugreifen, verfügt VMFS über eine festplatteninterne Sperrung.

Abbildung 1-3 zeigt mehrere ESX/ESXi-Systeme, die auf dasselbe VMFS-Volume zugreifen.

Abbildung 1-3. Gemeinsame Verwendung eines VMFS-Datenspeichers auf mehreren ESX/ESXi-Hosts



Da virtuelle Maschinen einen VMFS-Datenspeicher gemeinsam nutzen, kann es schwierig sein, Spitzenzugriffszeiten zu kennzeichnen oder die Leistung zu optimieren. Planen Sie den Speicherzugriff der virtuellen Maschinen zu Spitzenzeiten, und beachten Sie dabei, dass unterschiedliche Anwendungen verschiedene Spitzenzugriffszeiten aufweisen können. VMware empfiehlt einen Lastausgleich für die virtuellen Maschinen über Server, CPU und Speicher. Führen Sie auf jedem Server eine Kombination virtueller Maschinen aus, sodass nicht alle zur selben Zeit im selben Bereich einer hohen Nachfrage unterliegen.

Updates von Metadaten

Ein VMFS-Datenspeicher enthält Dateien der virtuellen Maschine, Verzeichnisse, symbolische Links, RDM-Deskriptor-Dateien usw. Der Datenspeicher verwaltet ebenfalls eine konsistente Ansicht aller Zuordnungsinformationen für diese Objekte. Diese Zuordnungsinformationen werden als Metadaten bezeichnet.

Metadaten werden jedes Mal aktualisiert, wenn auf die Atttribute einer Datei einer virtuellen Maschine zugegriffen wird oder diese anhand der folgenden Verfahren geändert werden:

- Erstellen, Erweitern oder Sperren einer Datei einer virtuellen Maschine.
- Ändern von Dateieigenschaften
- Ein- bzw. Ausschalten einer virtuellen Maschine

Entscheidungen zur Verwendung von LUNs

Bevor Sie LUNs mit einem VMFS-Datenspeicher formatieren, müssen Sie zunächst festlegen, wie Sie den Speicher für Ihre ESX/ESXi-Systeme einrichten möchten.

Bei der Wahl der richtigen Größe und Anzahl der zu verwendenden LUNs sollten Sie folgende Aspekte berücksichtigen:

- Jede LUN sollte über das richtige RAID-Level und die richtigen Speichermerkmale für die Anwendungen verfügen, die in virtuellen Maschinen ausgeführt werden, die die LUN verwenden.
- Eine LUN darf nur einen einzigen VMFS-Datenspeicher enthalten.
- Wenn mehrere virtuelle Maschinen auf dieselbe VMFS zugreifen, lassen sich mithilfe von Festplattenfreigaben Prioritäten für virtuelle Maschinen festlegen.

Die folgenden Gründe sprechen für weniger und dafür größere LUNs:

- Mehr Flexibilität beim Erstellen virtueller Maschinen, ohne beim Speicheradministrator mehr Speicherplatz anfordern zu müssen.
- Mehr Flexibilität bei der Größenänderung virtueller Festplatten, dem Erstellen von Snapshots usw.
- Weniger zu verwaltende VMFS-Datenspeicher.

Die folgenden Gründe sprechen für mehr und dafür kleinere LUNs:

- Weniger falsch genutzter Speicherplatz.
- Unterschiedliche Anwendungen könnten unterschiedliche RAID-Merkmale erfordern.
- Mehr Flexibilität, da die Multipathing-Richtlinie und gemeinsam genutzte Festplattenfreigaben pro LUN festgelegt werden.
- Für den Einsatz von Microsoft Clusterdienst muss jede Clusterfestplattenressource in ihrer eigenen LUN eingerichtet sein.
- Bessere Leistung aufgrund weniger Konflikte auf den einzelnen Volumes.

Wenn für eine virtuelle Maschine keine Speicherbeschreibung vorliegt, gibt es häufig keine einfache Methode zum Bestimmen der Anzahl und Größe der bereitzustellenden LUNs. Sie können experimentieren, indem Sie entweder ein Vorhersagemodell oder ein adaptives Modell verwenden.

Verwenden eines Vorhersagemodells zur richtigen LUN-Wahl

Wenn Sie Speicher für ESX/ESXi-Systeme einrichten, müssen Sie vor dem Erstellen von VMFS-Datenspeichern entscheiden, wie viele LUNs bereitgestellt werden sollen und welche Größe diese besitzen sollen. Sie können experimentieren, indem Sie das Vorhersagemodell verwenden.

Vorgehensweise

1 Stellen Sie mehrere LUNs mit unterschiedlichen Speichereigenschaften bereit.

2 Erstellen Sie einen VMFS-Datenspeicher in jeder LUN und benennen Sie jedes Volume entsprechend seinen Eigenschaften.

3 Erstellen Sie virtuelle Festplatten, um Kapazität für die Daten der Anwendungen virtueller Maschinen in den VMFS-Datenspeichern zu schaffen, die auf LUNs mit dem entsprechenden RAID-Level für die Anwendungsanforderungen erstellt wurden.

4 Verwenden Sie Festplattenfreigaben, um virtuelle Maschinen mit hoher Priorität von denen mit niedriger Priorität zu unterscheiden.

HINWEIS Festplattenfreigaben sind nur innerhalb eines bestimmten Hosts entscheidend. Die den virtuellen Maschinen auf einem Host zugeordneten Freigaben haben keine Auswirkungen auf virtuelle Maschinen auf anderen Hosts.

---

5 Sie führen die Anwendungen aus, um zu ermitteln, ob die Leistung der virtuellen Maschine zufriedenstellend ist.

Verwenden des adaptiven Modells zur richtigen LUN-Wahl

Wenn Sie Speicher für ESX/ESXi-Hosts einrichten, müssen Sie vor dem Erstellen von VMFS-Datenspeichern entscheiden, wie viele LUNs bereitgestellt werden sollen und welche Größe diese besitzen sollen. Sie können experimentieren, indem Sie das adaptive Modell verwenden.

Vorgehensweise

1 Stellen Sie eine große LUN (RAID 1+0 oder RAID 5) mit aktiviertem Schreibcache bereit.

2 Erstellen Sie in dieser LUN ein VMFS.

3 Erstellen Sie vier oder fünf virtuelle Festplatten im VMFS.

4 Führen Sie die Anwendungen aus, um zu ermitteln, ob die Festplattenleistung ausreichend ist.

Wenn die Leistung ausreicht, können Sie zusätzliche virtuelle Festplatten im VMFS einrichten. Reicht die Leistung nicht aus, haben Sie die Möglichkeit, eine neue, große LUN zu erstellen (eventuell mit einer anderen RAID-Ebene) und den Vorgang zu wiederholen. Verwenden Sie die Migrationsfunktion, damit keine Daten virtueller Maschinen bei der Neuerstellung der LUN verloren gehen.

Verwenden von Festplattenfreigaben zur Priorisierung virtueller Maschinen

Wenn mehrere virtuelle Maschinen auf denselben VMFS-Datenspeicher (und somit auf dieselbe LUN) zugreifen, lassen sich mithilfe von Festplattenfreigaben Prioritäten für virtuelle Maschinen festlegen. Bei Festplattenfreigaben wird zwischen virrtuellen Maschinen mit hoher und mit niedriger Priorität unterschieden.

Vorgehensweise

1 Starten Sie einen vSphere-Client und verbinden Sie ihn mit vCenter Server.

2 Wählen Sie die virtuelle Maschine im Bestandslistenbereich aus und klicken Sie im Menü auf **[Einstellungen der VM bearbeiten]** .

3 Klicken Sie auf die Registerkarte **[Ressourcen]** und anschließend auf **[Festplatte]** .

4 Klicken Sie mit der rechten Maustaste für die zu ändernde Festplatte auf die Spalte **[Anteile]** , und wählen Sie den erforderlichen Wert aus dem Dropdown-Menü aus.

   Der Anteilswert stellt die relative Metrik zur Steuerung der Festplattenbandbreite für alle virtuellen Maschinen dar. Die Werte **[Gering]** , **[Normal]** , **[Hoch]** und **[Benutzerdefiniert]** werden mit der Summe aller Anteile für alle virtuellen Maschinen auf dem Server und (bei ESX-Hosts) der Servicekonsole verglichen. Mit Symbolwerten für die Anteilszuweisung können Sie deren Konvertierung in numerische Werte konfigurieren.

5 Klicken Sie auf **[OK]** , um Ihre Auswahl zu speichern.

HINWEIS Festplattenfreigaben sind nur innerhalb eines bestimmten ESX/ESXi-Hosts entscheidend. Die den virtuellen Maschinen auf einem Host zugeordneten Freigaben haben keine Auswirkungen auf virtuelle Maschinen auf anderen Hosts.

Zugriff auf Daten in einem SAN durch virtuelle Maschinen

ESX/ESXi speichert Festplattendateien einer virtuellen Maschine in einem VMFS-Datenspeicher, der sich auf einem SAN-Speichergerät befindet. Sobald Gastbetriebssysteme der virtuellen Maschine SCSI-Befehle an die virtuellen Festplatten senden, übersetzt die SCSI-Virtualisierungsebene diese Befehle in VMFS-Dateivorgänge.

Wenn eine virtuelle Maschine mit seinen auf einem SAN gespeicherten virtuellen Festplatten interagiert, finden die folgenden Prozesse statt:

1 Wenn das Gastbetriebssystem in einer virtuellen Maschine zum Lesen oder Schreiben auf eine SCSI-Festplatte zugreifen muss, sendet dieses SCSI-Befehle an die virtuelle Festplatte.

2 Gerätetreiber im Betriebssystem der virtuellen Maschine kommunizieren mit den virtuellen SCSI-Controllern.

3 Der virtuelle SCSI-Controller leitet den Befehl an den VMkernel weiter.

4 Der VMkernel führt die folgenden Aufgaben aus.

- speichert die Datei im VMFS-Volume, das der Gastbetriebssystem-Festplatte der virtuellen Maschine entspricht.
- ordnet die Anforderungen für die Blöcke auf der virtuellen Festplatte den Blöcken auf dem entsprechenden physischen Gerät zu.
- sendet die geänderte E/A-Anforderung vom Gerätetreiber im VMkernel an den iSCSI-Initiator (Hardware oder Software).

5 Handelt es sich bei dem iSCSI-Initiator um einen Hardware-iSCSI-Adapter (unabhängig oder abhängig), führt der Adapter die folgenden Aufgaben aus.

- kapselt die E/A-Anforderungen in iSCSI-PDUs (Protocol Data Units).
- kapselt iSCSI-PDUs in TCP/IP-Pakete.
- sendet IP-Pakete über Ethernet an das iSCSI-Speichersystem.

6 Handelt es sich bei dem iSCSI-Initiator um einen Software-iSCSI-Adapter, findet der folgende Prozess statt.

- Der iSCSI-Initiator kapselt E/A-Anforderungen in iSCSI-PDUs.
- Der Initiator sendet SCSI-PDUs über TCP/IP-Verbindungen.
- Der VMkernel-TCP/IP-Stack gibt TCP/IP-Pakete an eine physische Netzwerkkarte weiter.
- Die physische Netzwerkkarte sendet IP-Pakete über Ethernet an das iSCSI-Speichersystem.

7 Abhängig davon, welchen Port der iSCSI-Initiator für die Verbindung zum Netzwerk verwendet, übermitteln Ethernet-Switches und Router die Anforderung an das Speichergerät, auf das der Host zugreifen möchte.

Grundlegendes zu Multipathing und Failover

Damit die Verbindung zwischen dem ESX/ESXi-Host und seinem Speicher nicht unterbrochen wird, unterstützt ESX/ESXi das so genannte Multipathing. Multipathing ist eine Technik, mit der Sie mehrere physische Pfade zur Übertragung von Daten zwischen dem Host und einem externen Speichergerät verwenden können.

Beim Ausfall eines beliebigen Elements im SAN-Netzwerk, z. B. eines Adapters, Switches oder Kabels, kann ESX/ESXi zu einem anderen physischen Pfad wechseln, der die Failover-Komponente nicht verwendet. Der Prozess des Wechselns zu einem anderen Pfad, um fehlgeschlagene Komponenten zu vermeiden, wird als Pfad-Failover bezeichnet.

Neben dem Pfad-Failover bietet Multipathing Lastausgleich. Lastausgleich ist der Vorgang zum Aufteilen der E/A-Lasten auf mehrere physische Pfade. Mit diesem Verfahren können potenzielle Engpässe reduziert oder vermieden werden.

HINWEIS Während eines Failovers kann es bei virtuellen Maschinen zu einer E/A-Verzögerung von bis zu sechs Sekunden kommen. Diese Verzögerung ist erforderlich, damit nach einer Topologieänderung ein stabiler Zustand des SAN hergestellt werden kann. Die E/A-Verzögerungen sind möglicherweise auf Aktiv/Passiv-Arrays länger und auf Aktiv-Aktiv-Arrays kürzer.

Verwalten mehrerer Pfade

Zur Verwaltung von Speicher-Multipathing verwendet ESX/ESXi eine spezielle VMkernel-Schicht: die Architektur des im laufenden Betrieb austauschbaren Speichers (Pluggable Storage Architecture, PSA). PSA stellt ein offenes, modulares Framework dar, das die gleichzeitige Ausführung von mehreren Multipathing-Plug-Ins (MPPs) koordiniert.

Das von ESX/ESXi standardmäßig bereitgestellte VMkernel-Multipathing-Plug-In ist das NMP (VMware Native Multipathing Plug-In). Das NMP ist ein erweiterbares Modul zur Verwaltung von Sub-Plug-Ins. Das NMP-Modul verwaltet zwei Sub-Plug-In-Typen: die Plug-Ins für Speicher-Array-Typen (SATPs) und die Pfadauswahl-Plug-Ins (PSPs). SATPs und PSPs können von VMware bereitgestellt und integriert oder durch einen Drittanbieter zur Verfügung gestellt werden.

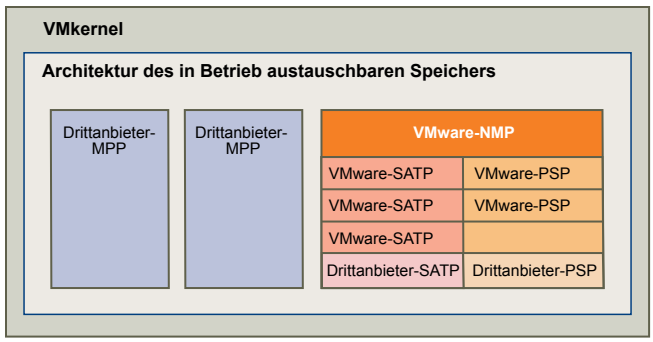
Wenn mehr Multipathing-Funktionen erforderlich sind, kann ein Drittanbieter MPP zusätzlich oder als Ersatz für das Standard-NMP bereitstellen.

Bei der Koordination vom VMware NMP und ggf. installierter Drittanbieter-MPPs führt PSA die folgenden Aufgaben aus:

- Laden und Entladen von Multipathing-Plug-Ins.
- Verbergen von Angaben zur virtuellen Maschine vor einem bestimmten Plug-In.
- Weiterleiten von E/A-Anforderungen für ein bestimmtes logisches Gerät an das MPP, das das Gerät verwaltet.
- Verarbeiten der E/A-Warteschlangen für logische Geräte.
- Implementieren der gemeinsamen Nutzung der Bandbreite für logische Geräte durch virtuelle Maschinen.
- Verarbeiten der E/A-Warteschlangen für physische Speicher-HBAs.
- Verarbeiten der Erkennung und Entfernung physischer Pfade.
- Bereitstellen von E/A-Statistiken für logische Geräte und physische Pfade.

Wie unter Abbildung 1-4 beschrieben, kann mehrere Drittanbieter-MPPs parallel zum VMware NMP ausgeführt werden. Wenn sie installiert sind, ersetzen die Drittanbieter-MPPs das Verhalten des NMP und übernehmen die gesamte Steuerung des Pfad-Failovers und der Lastausgleichs-Vorgänge für die angegebenen Speichergeräte.

Abbildung 1-4. Architektur des im Betrieb austauschbaren Speichers



Mit den Multipathing-Modulen werden die folgenden Verfahren ausgeführt:

- Verwalten des Beanspruchens und Freigebens physischer Pfade.
- Verwalten der Erstellung, Registrierung und der Aufhebung der Registrierung von logischen Geräten.
- Zuordnen physischer Pfade zu logischen Geräten.
- Unterstützung der Erkennung und Behebung von nicht verfügbaren Pfaden.
- Verarbeiten von E/A-Anforderungen an logische Geräte:
  - Auswahl eines optimalen physischen Pfades für die Anforderung.
  - Je nach Speichergerät Ausführen bestimmter Aktionen, die zur Verarbeitung von Pfadfehlern und Wiederholungsversuchen für E/A-Befehle notwendig sind.
- Unterstützen von Verwaltungsaufgaben, wie z. B. dem Abbrechen oder Zurücksetzen von logischen Geräten.

VMware Multipathing-Modul

Standardmäßig bietet ESX/ESXi ein erweiterbares Multipathing-Modul, das als NMP (Natives Multipathing-Plug-In) bezeichnet wird.

Das VMware NMP unterstützt normalerweise alle in der VMware Speicher-HCL aufgeführten Speicher-Arrays und bietet einen auf dem Array-Typ basierenden Pfadauswahl-Algorithmus. Das NMP weist einem bestimmten Speichergerät oder einer bestimmten LUN mehrere physische Pfade zu. Die jeweiligen Details der Verarbeitung eines Pfad-Failovers für ein bestimmtes Speicher-Array werden an ein Speicher-Array-Typ-Plug-In (SATP) delegiert. Die jeweiligen Details zum Festlegen des physischen Pfads, der zum Ausgeben einer E/A-Anforderung an ein Speichergerät verwendet wird, werden von einem Pfadauswahl-Plug-In (Path Selection Plug-In, PSP) verarbeitet. SATPs und PSPs sind Sub-Plug-Ins innerhalb des NMP-Moduls.

Bei der Installation von ESX/ESXi wird automatisch das entsprechende SATP für ein von Ihnen verwendetes Array installiert. Sie müssen keine SATPs beschaffen oder herunterladen.

VMware SATPs

Plug-Ins für Speicher-Array-Typen (SATPs) werden in Verbindung mit dem VMware NMP ausgeführt und übernehmen arrayspezifische Vorgänge.

ESX/ESXi bietet ein SATP für jeden von VMware unterstützten Array-Typ. Außerdem werden Standard-SATPs für nicht-spezifische Aktiv/Aktiv- und ALUA-Speicher-Arrays und das lokale SATP für direkt angeschlossene Geräte zur Verfügung gestellt. Jedes SATP enthält spezielle Merkmale einer bestimmten Klasse von Speicher-Arrays und kann die arrayspezifischen Vorgänge ausführen, die zum Ermitteln des Pfadstatus und zum Aktivieren eines inaktiven Pfads erforderlich sind. Daher kann das NMP-Modul selbst mit mehreren Speicher-Arrays arbeiten, ohne die Angaben zu den Speichergeräten zu kennen.

Nachdem das NMP ermittelt, welches SATP für ein bestimmtes Speichergerät verwendet werden muss, und das SATP physischen Pfaden für dieses Speichergerät zuweist, implementiert das SATP die folgenden Aufgaben:

- Überwachung des Status der einzelnen physischen Pfade.
- Melden von Änderungen des Status der einzelnen physischen Pfade.
- Ausführen von für das Speicher-Failover erforderlichen arrayspezifischen Aktionen. Beispielsweise können für Aktiv/Passiv-Geräte passive Pfade aktiviert werden.

VMware PSPs

Pfadauswahl-Plug-Ins (PSPs) werden mit dem VMware-NMP ausgeführt und sind verantwortlich für die Auswahl eines physischen Pfads für E/A-Anforderungen.

Das VMware NMP weist auf der Grundlage des SATP, das den physischen Pfaden für das jeweilige Gerät zugeordnet ist, ein Standard-PSP für jedes logische Gerät zu. Sie können das Standard-PSP außer Kraft setzen.

Standardmäßig unterstützt VMware NMP die folgenden PSPs:

Zuletzt verwendet (VMW_PSP_MRU)
Wählt den Pfad aus, den der ESX/ESXi-Host zuletzt verwendet hat, um auf ein bestimmtes Gerät zuzugreifen. Wenn dieser Pfad nicht verfügbar ist, wechselt der Host zu einem anderen Pfad und verwendet weiterhin den neuen Pfad, wenn dieser verfügbar ist. MRU ist die Standard-Pfadrichtlinie für Aktiv/Passiv-Arrays.

Feststehend (VMW_PSP_FIXED)
Verwendet den festgelegten bevorzugten Pfad, wenn dieser konfiguriert wurde. Anderenfalls wird der erste funktionierende Pfad verwendet, der beim Systemstart ermittelt wird. Wenn der Host den bevorzugten Pfad nicht verwenden kann, trifft er eine zufällige Auswahl für einen alternativen verfügbaren Pfad. Sobald der bevorzugte Pfad verfügbar ist, kehrt der Host zu diesem zurück. Feststehend (Fixed) ist die Standard-Pfadrichtlinie für Aktiv/Aktiv-Arrays.

Vorsicht Wenn die Pfadrichtlinie **[Feststehend]** mit Aktiv/Passiv-Arrays verwendet wird, kann sie Pfad-Thrashing hervorrufen.

VMW_PSP_FIXED_AP
Erweitert die Funktionalität der Pfadrichtlinie „Feststehend“ auf Aktiv/Passiv- und ALUA-Modus-Arrays.

Round Robin (VMW_PSP_RR)
Verwendet einen Pfadauswahlalgorithmus, bei dem eine Rotation unter Berücksichtigung aller verfügbaren aktiven Pfade stattfindet und ein pfadübergreifender Lastausgleich ermöglicht wird.

NMP-E/A-Ablauf von VMware

Wenn eine virtuelle Maschine eine E/A-Anforderung an ein vom NMP verwaltetes Speichergerät ausgibt, läuft der folgende Prozess ab.

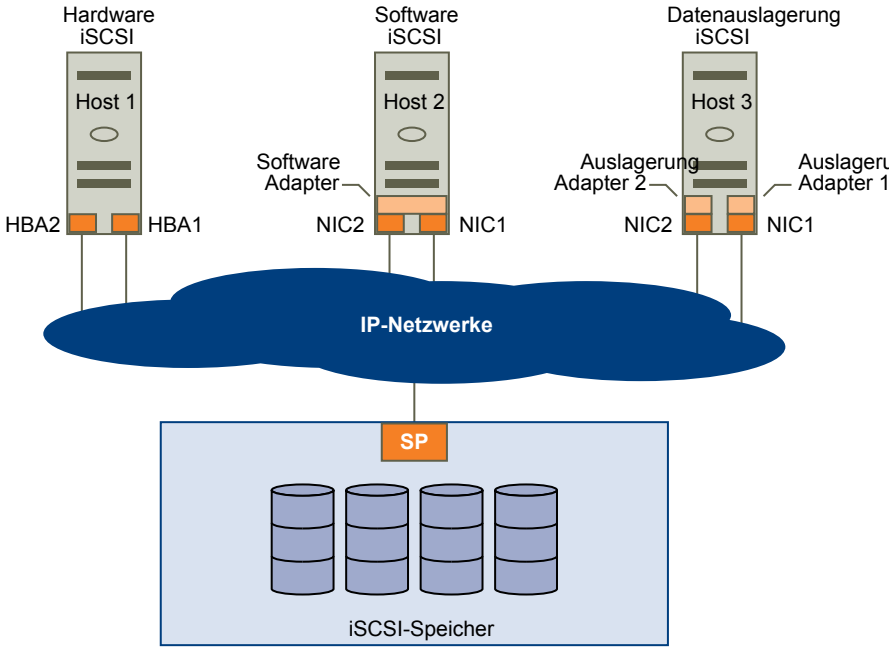
1. Das NMP ruft das PSP auf, das diesem Speichergerät zugewiesen ist.
2. Das PSP wählt einen entsprechenden physischen Pfad für die zu sendende E/A.
3. Das NMP gibt die E/A-Anforderung auf dem vom PSP gewählten Pfad aus.
4. Wenn der E/A-Vorgang erfolgreich ist, meldet das NMP dessen Abschluss.
5. Wenn der E/A-Vorgang einen Fehler meldet, ruft das NMP das entsprechende SATP auf.
6. Das SATP interpretiert die E/A-Fehlercodes und aktiviert ggf. die inaktiven Pfade.
7. Das PSP wird aufgerufen, um einen neuen Pfad für das Senden der E/A zu wählen.

Hostbasiertes Pfad-Failover

Beim Einrichten Ihres ESX/ESXi-Hosts für das Multipathing und das Failover können Sie je nach Typ der iSCSI-Initiatoren auf Ihrem Host mehrere iSCSI-HBAs oder mehrere Netzwerkkarten verwenden.

Abbildung 1-5 zeigt Multipathing-Setups, die mit verschiedenen Typen von iSCSI-Initiatoren möglich sind.

Abbildung 1-5. Hostbasiertes Pfad-Failover



Failover mit Hardware-iSCSI

Beim Hardware-iSCSI sind auf dem Host in der Regel zwei oder mehr Hardware-iSCSI-Adapter verfügbar, über die das Speichersystem mithilfe von einem oder mehreren Switches erreicht werden kann. Alternativ könnte das Setup auch einen Adapter und zwei Speicherprozessoren umfassen, sodass der Adapter einen anderen Pfad verwenden kann, um das Speichersystem zu erreichen.

In der Abbildung Abbildung 1-5 hat Host1 zwei Hardware-iSCSI-Adapter, HBA1 und HBA2, die zwei physische Pfade zum Speichersystem zur Verfügung stellen. Multipathing-Plug-Ins auf dem Host, ob VMkernel-NMP oder Drittanbieter-MPPs, haben standardmäßig Zugriff auf die Pfade und können den Status der einzelnen physischen Pfade überwachen. Wenn beispielsweise HBA1 oder die Verknüpfung zwischen HBA1 und dem Netzwerk fehlschlägt, können Mehrfachpfad-Plug-Ins den Pfad auf HBA2 wechseln.

Failover mit Software-iSCSI

Mit Software-iSCSI können Sie, wie bei Host 2 der Abbildung Abbildung 1-5 dargestellt, mehrere Netzwerkkarten verwenden, die Failover- und Lastausgleichsfunktionen für iSCSI-Verbindungen zwischen dem Host und Speichersystemen bieten.

Da Multipathing-Plug-Ins keinen direkten Zugriff auf die physischen Netzwerkkarten auf Ihrem Host haben, müssen Sie dazu zuerst jede einzelne physische Netzwerkkarte mit einem separaten VMkernel-Port verbinden. Danach verbinden Sie mithilfe einer Port-Bindungstechnik alle VMkernel-Ports mit dem Software-iSCSI-Initiator. Somit erhält jeder VMkernel-Port, der mit einer separaten NIC verbunden ist, einen anderen Pfad, der vom iSCSI-Speicherstapel und dessen speicherfähigen Mehrfachpfad-Plug-Ins verwendet werden kann.

Informationen zur Konfiguration von Multipathing für das Software-iSCSI finden Sie unter „Netzwerkkonfiguration für Software-iSCSI und abhängige Hardware-iSCSI“, auf Seite 39.

Array-basiertes Failover

Die Pfadnutzung der Ports wird von einigen iSCSI-Speichersystemen automatisch und für ESX/ESXi transparent verwaltet.

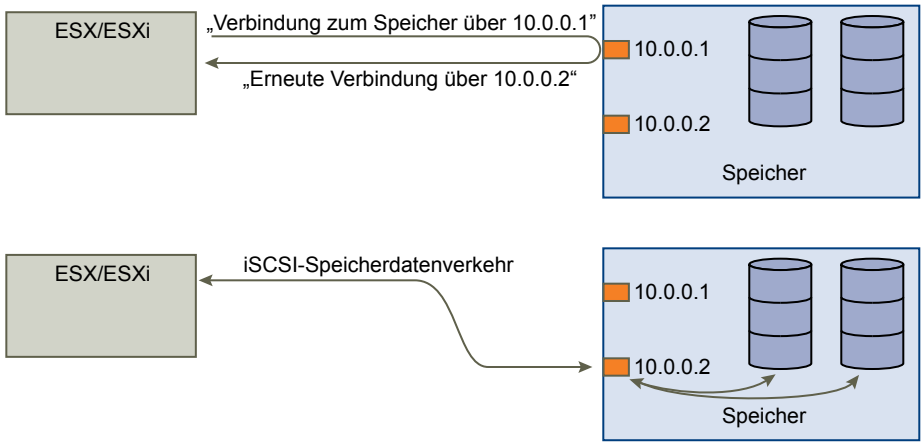
Bei Verwendung eines dieser Speichersysteme werden für den ESX/ESXi-Host nicht mehrere Ports im Speicher angezeigt, daher kann er den Speicherport für die Verbindung nicht wählen. Diese Systeme verfügen über eine einzige virtuelle Portadresse, über die ESX/ESXi anfangs kommuniziert. Während dieser ersten Kommunikation kann ESX/ESXi vom Speichersystem zu einem anderen Port im Speichersystem umgeleitet werden, um dann mit diesem zu kommunizieren. Der iSCSI-Initiator in ESX/ESXi folgt dieser erneuten Verbindungsanforderung und stellt eine Verbindung mit einem anderen Port im System her. Mithilfe dieser Methode wird die Last durch das Speichersystem auf alle verfügbaren Ports verteilt.

Wird die Verbindung zwischen ESX/ESXi und einem dieser Ports unterbrochen, wird automatisch eine neue Verbindung mit dem virtuellen Port des Speichersystems aufgebaut und zu einem aktiven, verwendbaren Port umgeleitet. Das Wiederherstellen und Umleiten dieser Verbindung geschieht schnell und führt in der Regel zu keiner Unterbrechung der ausgeführten virtuellen Maschinen. Darüber hinaus können diese Speichersysteme anfordern, dass iSCSI-Initiatoren die Verbindung zum System wiederherstellen, um den Speicherport zu wechseln, mit dem sie verbunden sind. Auf diese Weise lassen sich mehrere Ports am effektivsten nutzen.

Abbildung 1-6 zeigt ein Beispiel für eine Portumleitung. ESX/ESXi versucht die Verbindung zum virtuellen Port 10.0.0.1 herzustellen. Das Speichersystem leitet diese Anforderung an 10.0.0.2 weiter. ESX/ESXi stellt eine Verbindung mit 10.0.0.2 her und verwendet diesen Port für die E/A-Kommunikation.

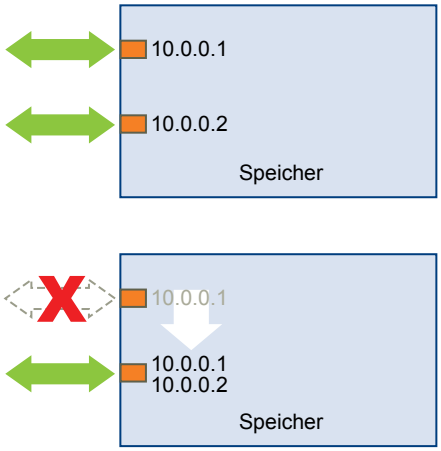
HINWEIS Verbindungen werden nicht immer vom Speichersystem umgeleitet. Der Port bei 10.0.0.1 könnte ebenfalls für Datenverkehr genutzt werden.

Abbildung 1-6. Portumleitung



Wenn der Port im Speichersystem, der als virtueller Port fungiert, nicht mehr verfügbar ist, wird die Adresse des virtuellen Ports durch das Speichersystem einem anderen Port im System zugewiesen. Abbildung 1-7 veranschaulicht ein Beispiel zu dieser Art von Neuzuweisung eines Ports. Hierbei fällt der virtuelle Port 10.0.0.1 aus und die IP-Adresse des virtuellen Ports wird einem anderen Port zugewiesen. Der zweite Port antwortet auf beide Adressen.

Abbildung 1-7. Neuzuweisung von Ports



Es kann bei einem arraybasierten Failover nur dann mehrere Pfade zum Speicher geben, wenn Sie mehrere Ports auf dem ESX/ESXi-Host verwenden. Diese Pfade sind Aktiv/Aktiv. Weitere Informationen finden Sie unter „iSCSI-Sitzungsverwaltung“, auf Seite 54.

Auswählen von Speicherorten für virtuelle Maschinen

Bei der Leistungsoptimierung der virtuellen Maschinen ist der Speicherort ein wichtiger Faktor. Es muss stets zwischen kostenintensivem Speicher, der eine optimale Leistung und hohe Verfügbarkeit bietet, und kostengünstigem Speicher mit niedrigerer Leistung abgewogen werden.

Die Speichereinteilung in verschiedene Qualitätsstufen ist von zahlreichen Faktoren abhängig:

- Hoch. Bietet hohe Leistung und Verfügbarkeit. Bietet unter Umständen auch integrierte Snapshots, um Sicherungen und PiT-Wiederherstellungen (Point-in-Time) zu vereinfachen. Unterstützt Replikationsfunktionen, vollständige SP-Redundanz und SAS-Laufwerke. Verwendet teure Spindeln.
- Mittel. Bietet durchschnittliche Leistung, niedrigere Verfügbarkeit, geringe SP-Redundanz und SCSI- bzw. SAS-Laufwerke. Bietet möglicherweise Snapshots. Verwendet Spindeln mit durchschnittlichen Kosten.
- Niedrig. Bietet niedrige Leistung, geringe interne Speicherredundanz. Verwendet kostengünstige SCSI-Laufwerke oder SATA (serielle kostengünstige Spindeln).

Nicht alle Anwendungen müssen auf dem Speicher mit der höchsten Leistung und Verfügbarkeit ausgeführt werden – zumindest nicht während ihres gesamten Lebenszyklus.

Hinweis Wenn Sie einige der von hochwertigen Speichern bereitgestellten Funktionen, z. B. Snapshots, benötigen, die Kosten aber gering halten möchten, können Sie die gewünschten Funktionen eventuell über den Einsatz von Software erreichen. Beispielsweise können Sie Snapshots auch mit einer Software erstellen.

Bevor Sie entscheiden, wo Sie eine virtuelle Maschine platzieren möchten, sollten Sie sich die folgenden Fragen stellen:

- Wie wichtig ist die virtuelle Maschine?
- Welche Leistungs- und Verfügbarkeitsanforderungen gelten für sie?
- Welche PiT-Wiederherstellungsanforderungen gelten für sie?
- Welche Sicherungsanforderungen gelten für sie?
- Welche Wiederherstellungsanforderungen gelten für sie?

Die Einstufung einer virtuellen Maschine kann während ihres Lebenszyklus wechseln, z. B. wenn Prioritäten oder Technologien geändert wurden, die eine höhere oder niedrigere Einstufung zur Folge haben. Die Wichtigkeit ist relativ und kann sich aus verschiedenen Gründen ändern, z. B. bei Änderungen im Unternehmen, betriebswirtschaftlichen Abläufen, gesetzlichen Anforderungen oder Erstellung eines Notfallplans.

Vorbereitung auf einen Serverausfall

Die RAID-Architektur von SAN-Speichern schützt an sich vor Ausfällen auf physischer Festplattenebene. Ein SAN stellt mehrere Pfade zwischen Servern und Speicher bereit, die vor Netzwerk- und Portausfällen schützen. Der letzte Schritt zu einer ausfallsicheren Umgebung ist ein Schutz vor Serverausfällen.

Verwenden von VMware HA

Eine der von ESX/ESXi bieteten Failover-Optionen ist VMware High Availability (HA).

VMware HA ermöglicht die Einteilung virtueller Maschinen in Failover-Gruppen. Bei einem Hostausfall werden alle verknüpften virtuellen Maschinen in den Gruppen umgehend auf anderen Hosts neu gestartet. Wenn eine virtuelle Maschine auf einem anderen Host wiederhergestellt wird, geht zwar der zugehörige Speicherstatus verloren, aber der Festplattenstatus vor dem Hostausfall bleibt erhalten (absturzkonsistentes Failover). Für HA wird ein gemeinsam genutzter Speicher (z. B. ein SAN) benötigt.

HINWEIS Wenn Sie VMware HA verwenden möchten, müssen Sie über eine entsprechende Lizenz verfügen.

Server-Failover und Überlegungen zum Speicher

Wenn Sie Ihren ESX/ESXi-Host für den Einsatz in Verbindung mit einem SAN konfigurieren, müssen Sie eine ausfallsichere Umgebung schaffen und Schutz vor Serverausfällen bieten.

Für jede Art von Server-Failover müssen bestimmte Aspekte in Betracht gezogen werden:

- Die Server-Failover-Verfahren funktionieren nur dann, wenn jeder Server auf denselben Speicher zugreifen kann. Da für mehrere Server viel Festplattenspeicherplatz erforderlich ist und Failover-Verfahren für das Speichersystem des Servers ergänzen, werden SANs normalerweise in Verbindung mit Server-Failover eingesetzt.
- Wenn Sie ein SAN einrichten, sodass es ein Server-Failover unterstützt, müssen alle Datenspeicher, die von virtuellen Maschinen in Clustern verwendet werden, für alle ESX/ESXi-Hosts sichtbar sein.

  Obwohl ein Datenspeicher für einen Host verfügbar ist, müssen nicht unbedingt alle virtuellen Maschinen auf diesem Host auf alle Daten des Datenspeichers zugreifen können. Der Zugriff einer virtuellen Maschine ist nur auf die virtuellen Festplatten möglich, für die sie konfiguriert wurde. Virtuelle Festplatten werden im Falle eines Konfigurationsfehlers gesperrt, sobald die virtuelle Maschine gestartet wird, um so Datenbeschädigungen zu vermeiden.

HINWEIS Als Regel gilt: Beim Starten über ein SAN sollte jedes Start-Volume ausschließlich für den Host sichtbar sein, der von diesem Volume gestartet wird. Es sei denn, Sie führen eine Wiederherstellung nach einem Ausfall durch, indem Sie einn zweiten Host mit demselben Volume verknüpfen. In diesem Fall wird das betreffende SAN-Volume nicht tatsächlich über ein SAN gestartet. Da es beschädigt ist, wird kein Host darüber gestartet. Das SAN-Volume ist ein reguläres, nicht startfähiges Volume, das für einen Host sichtbar ist.

LUN-Anzeige und erneutes Prüfen

Ein SAN ist dynamisch und die für einen bestimmten Host verfügbaren LUNs können durch verschiedene Faktoren geändert werden.

Beim Starten erkennt der VMkernel die LUNs, die anschließend im vSphere-Client angezeigt werden. Wenn Sie Änderungen an den LUNs vorgenommen haben, müssen Sie eine erneute Prüfung durchführen, damit die Änderungen wirksam werden.

- Neu erstellte LUNs im iSCSI-Speicher
- Änderungen an der LUN-Zugriffssteuerung
- Änderungen an der Verbindung

Konfigurieren von iSCSI-Initiatoren und -Speicher

2

Bevor Sie ESX/ESXi in einem SAN verwenden können, müssen Sie die iSCSI-Initiatoren und -Speicher installieren.

Hierzu müssen Sie zunächst bestimmte Grundanforderungen und dann die empfohlenen Vorgehensweisen zum Installieren und Einrichten von Hardware- oder Software-iSCSI-Initiatoren beachten, um auf das SAN zuzugreifen.

Dieses Kapitel behandelt die folgenden Themen:

- „Anforderungen an ESX/ESXi-iSCSI-SAN“, auf Seite 32
- „Beschränkungen für ESX/ESXi-iSCSI-SAN“, auf Seite 32
- „Festlegen der LUN-Zuordnungen“, auf Seite 32
- „Netzwerkkonfiguration und Authentifizierung“, auf Seite 33
- „Einrichten von unabhängigen Hardware-iSCSI-Adaptern“, auf Seite 33
- „Einrichten und Konfigurieren von abhängigen Hardware-iSCSI-Adaptern“, auf Seite 35
- „Einrichten und Konfigurieren des Software-iSCSI-Adapters“, auf Seite 37
- „Netzwerkkonfiguration für Software-iSCSI und abhängige Hardware-iSCSI“, auf Seite 39
- „Binden von iSCSI-Ports an iSCSI-Adapter“, auf Seite 43
- „Verwenden von Jumbo-Frames mit iSCSI“, auf Seite 45
- „Aktivieren von Jumbo-Frames für Software-iSCSI und abhängige Hardware-iSCSI“, auf Seite 45
- „Konfigurieren von Erkennungsadressen für iSCSI-Initiatoren“, auf Seite 46
- „Konfigurieren von CHAP-Parametern für iSCSI-Adapter“, auf Seite 48
- „Konfigurieren zusätzlicher Parameter für iSCSI“, auf Seite 52
- „iSCSI-Sitzungsverwaltung“, auf Seite 54
- „Hinzufügen von iSCSI-Speicher“, auf Seite 56

Anforderungen an ESX/ESXi-iSCSI-SAN

Vor der ordnungsgemäßen Verwendung eines ESX/ESXi-Hosts mit einem SAN müssen bestimmte Anforderungen erfüllt sein.

- Stellen Sie sicher, dass die Hardware- und Firmware-Kombinationen für Ihren SAN-Speicher in Verbindung mit ESX/ESXi-Systemen unterstützt werden. Eine aktuelle Liste finden Sie im Abschnitt „Speicher/SAN“ des online verfügbaren *Hardware-Kompatibilitätshandbuch*.
- Konfigurieren Sie Ihr System so, dass nur ein VMFS-Datenspeicher für jede LUN vorhanden ist. In VMFS-3 muss die Erreichbarkeit nicht festgelegt werden.
- Wenn Sie keine Server ohne Festplatte verwenden (die über ein SAN gestartet werden), dürfen Sie keine Diagnosepartition auf einer SAN-LUN einrichten. Sollten Sie jedoch Server ohne Festplatte verwenden, die über ein SAN gestartet werden, ist eine gemeinsame Diagnosepartition angebracht.
- Verwenden Sie RDMs für den Zugriff auf eine beliebige Raw-Festplatte.
- Installieren Sie den SCSI Controller-Treiber im Gastbetriebssystem, damit Sie eine ausreichende Größe der Warteschlange festlegen können. Die Warteschlangentiefe für den physischen HBA können Sie während der Systeminstallation festlegen.
- Erhöhen Sie den Wert des SCSI-Parameters `TimeoutValue` für virtuelle Maschinen, auf denen Microsoft Windows ausgeführt wird, damit Windows aus Pfad-Failover resultierende E/A-Verzögerungen besser toleriert.

Beschränkungen für ESX/ESXi-iSCSI-SAN

In diesem Thema werden die Beschränkungen bei der Verwendung von ESX/ESXi mit einem iSCSI SAN aufgelistet.

- ESX/ESXi unterstützt keine über iSCSI verbundenen Bandlaufwerke.
- Sie können keine Multipathing-Software für virtuelle Maschinen verwenden, um einen E/A-Lastausgleich für eine einzelne physische LUN durchzuführen.
- Ein Host kann nicht auf dieselbe LUN zugreifen, wenn er gleichzeitig abhängige und unabhängige Hardware-iSCSI-Adapter nutzt.

Festlegen der LUN-Zuordnungen

Wennn Sie Ihr ESX/ESXi-System zur Verwendung des iSCSI SAN-Speichers vorbereiten, müssen Sie zunächst LUN-Zuordnungen vornehmen.

Beachten Sie Folgendes:

- Speicherbereitstellung. Damit das ESX-System die LUNs beim Start erkennt, müssen alle iSCSI-Speicherziele so konfiguriert werden, dass Ihr Host darauf zugreifen und sie verwenden kann. Konfigurieren Sie Ihren Host auch in der Weise, dass er alle verfügbaren iSCSI-Ziele erkennen kann.
- VMotion und VMware DRS. Wenn Sie vCenter Server und VMotion oder DRS verwenden, sollten Sie sicherstellen, dass die LUNs für die virtuellen Maschinen allen ESX/ESXi-Hosts bereitgestellt werden. Diese Konfiguration bietet die höchste Flexibilität beim Verschieben virtueller Maschinen.
- Aktiv/Aktiv- im Vergleich zu Aktiv/Passiv-Arrays. Bei der Verwendung von VMotion oder DRS mit einem SAN-Speichergerät vom Typ „Aktiv/Passiv“ sollten Sie sicherstellen, dass alle ESX/ESXi-Systeme über einheitliche Pfade zu allen Speicherprozessoren verfügen. Anderenfalls kann es bei VMotion-Migrationen zu einem Pfad-Thrashing kommen.

Für Aktiv/Passiv-Speicher-Arrays, die nicht im Abschnitt „Speicher/SAN“ des online verfügbaren VMware-Kompatibilitätshandbuchs aufgelistet sind, wird von VMware kein Speicherport-Failover unterstützt. Sie müssen den Server am aktiven Port des Speichersystems anschließen. Durch diese Konfiguration wird sichergestellt, dass die LUNs dem ESX/ESXi-Host angezeigt werden.

Netzwerkkonfiguration und Authentifizierung

Bevor Ihr ESX/ESXi den iSCSI-Speicher erkennen kann, müssen die iSCSI-Initiatoren konfiguriert werden und die Einrichtung der Authentifizierung ist möglicherweise erforderlich.

- Für Software- und abhängiges Hardware-iSCSI muss die Vernetzung für den VMkernel konfiguriert werden. Mit dem Dienstprogramm `vmkping` können Sie die Netzwerkkonfiguration überprüfen. Für den Einsatz von Hardware-iSCSI müssen HBA-Netzwerkparameter wie IP-Adresse, Subnetzmaske und Standard-Gateway konfiguriert werden.
- Überprüfen und ändern Sie ggf. den standardmäßigen Initiator-Namen.
- Die Erkennungsadresse des Speichersystems muss angegeben werden. Zudem sollte ein Ping-Signal über `vmkping` an die Adresse gesendet werden können.
- Um die CHAP-Authentifizierung zu verwenden, aktivieren Sie diese auf Seiten des Initiators und des Speichersystems. Nach dem Aktivieren der Authentifizierung gilt diese ausschließlich für alle Ziele, die noch nicht erkannt wurden (nicht aber für bereits erkannte Ziele). Wurde schließlich die Erkennungsadresse festgelegt, werden die neu erkannten Ziele angezeigt und können verwendet werden.

Weitere Informationen zur Verwendung des Befehls `vmkping` finden Sie in der VMware-Knowledgebase.

Einrichten von unabhängigen Hardware-iSCSI-Adaptern

Ein unabhängiger Hardware-iSCSI-Adapter ist ein spezielle Adapter von Drittanbietern, die über TCP/IP auf iSCSI-Speicher zugreifen kann. Dieser iSCSI-Adapter steuert die gesamte iSCSI- und Netzwerk-Verarbeitung und -Verwaltung für Ihr ESX/ESXi-System.

Der Installations- und Konfigurationsprozess für die unabhängigen Hardware-iSCSI-Adapter umfasst dieses Schritte:

1 Prüfen Sie, ob der Adapter lizenziert werden muss.

  Informationen finden Sie in der Dokumentation des Anbieters.

2 Installieren Sie den Adapter.

  Weitere Informationen zur Installation finden Sie in der Herstellerdokumentation.

3 Stellen Sie sicher, dass der Adapter ordnungsgemäß installiert wurde.

  Siehe „Anzeigen von unabhängigen Hardware-iSCSI-Adaptern“, auf Seite 34.

4 Erkennungsadressen konfigurieren.

  Siehe „Konfigurieren von Erkennungsadressen für iSCSI-Initiatoren“, auf Seite 46.

5 CHAP-Parameter konfigurieren.

  Siehe „Konfigurieren von CHAP-Parametern für iSCSI-Adapter“, auf Seite 48.

Sie müssen den Hardware-iSCSI-Adapter installieren und die Erkennungsadressen- und CHAP-Parameter konfigurieren, damit Ihr Host auf das iSCSI-Speichergerät zugreifen kann.

Anzeigen von unabhängigen Hardware-iSCSI-Adaptern

Zeigen Sie einen Hardware-iSCSI-Adapter an, um zu überprüfen, ob er korrekt installiert und konfigurationsbereit ist.

Voraussetzungen

Nachdem Sie einen Hardware-iSCSI-Adapter installiert haben, wird er in der Liste der Speicheradapter angezeigt, die zum Konfigurieren zur Verfügung stehen. Seine Eigenschaften können angezeigt werden.

Erforderliche Berechtigung:**Host.Konfiguration.Konfiguration für Speicherpartition**

Vorgehensweise

1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Host.

2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend unter **[Hardware]** auf **[Speicheradapter]** .

Falls installiert, sollte der Hardware-iSCSI-Initiator in der Liste der Speicheradapter angezeigt werden.

3 Wählen Sie den anzuzeigenden Initiator aus.

Die standardmäßigen Details für den Initiator werden angezeigt, darunter das Modell, der iSCSI-Name, iSCSI-Alias, IP-Adresse sowie Ziel- und Pfadinformationen.

4 Klicken Sie auf **[Eigenschaften]** .

Das Dialogfeld **[iSCSI-Initiator-Eigenschaften (iSCSI Initiator Properties)]** wird angezeigt. Auf der Registerkarte **[Allgemein (General)]** werden zusätzliche Merkmale des Initiators angezeigt.

Sie können den Hardware-Initiator jetzt konfigurieren oder seine Standardmerkmale ändern.

Ändern des Namens und der IP-Adresse für unabhängige Hardware-Initiatoren

Stellen Sie beim Konfigurieren der unabhängigen Hardware-iSCSI-Initiatoren sicher, dass ihre Namen und IP-Adressen ordnungsgemäß formatiert sind.

Vorgehensweise

1 Greifen Sie auf das Dialogfeld „Eigenschaften des iSCSI-Initiators“ zu.

2 Klicken Sie auf **[Konfigurieren]** .

3 Um den Standard-iSCSI-Namen für den Initiator zu ändern, geben Sie einen neuen Namen ein.

Stellen Sie sicher, dass der eingegebene Name weltweit eindeutig und ordnungsgemäß formatiert ist, anderenfalls wird der Hardware-iSCSI-Initiator möglicherweise von bestimmten Speichergeräten nicht erkannt.

4 (Optional) Geben Sie das iSCSI-Alias ein.

Das Alias ist ein Name, der zur Identifizierung des Hardware-iSCSI-Initiators verwendet wird.

5 Ändern Sie die Standard-IP-Einstellungen.

Sie müssen die Standard-IP-Einstellungen ändern, damit diese für das IP-SAN ordnungsgemäß konfiguriert sind. Wenden Sie sich an Ihren Netzwerkadministrator, um die IP-Einstellung für den HBA zu erfahren.

6 Klicken Sie auf **[OK]** , um Ihre Änderungen zu speichern.

Wenn Sie den iSCSI-Namen ändern, wird er für neue iSCSI-Sitzungen verwendet. In vorhandenen Sitzungen werden neue Einstellungen nicht verwendet. Sie treten erst bei erneuter Anmeldung in Kraft.

Einrichten und Konfigurieren von abhängigen Hardware-iSCSI-Adaptern

Ein abhängiger Hardware-iSCSI-Adapter ist ein Drittanbieter-Adapter, der vom VMware-Netzwerk sowie von den iSCSI-Konfigurations- und -Verwaltungsschnittstellen abhängt, die von VMware zur Verfügung gestellt werden.

Bei diesem Adaptertyp kann es sich um eine Karte (z. B. eine Broadcom 5709-Netzwerkkarte) handeln, die einen Standard-Netzwerkadapter und die iSCSI-Offload-Funktion für denselben Port bietet. Die iSCSI-Offload-Funktion wird als iSCSI-Adapter in der Liste der Speicheradapter angezeigt. Obwohl der iSCSI-Adapter standardmäßig aktiviert ist, müssen Sie, damit er funktionsbereit ist, eine Vernetzung für den iSCSI-Datenverkehr einrichten und den Adapter und einen entsprechenden VMkernel-iSCSI-Port binden. Anschließend können Sie den Adapter konfigurieren.

Der gesamte Installations- und Konfigurationsprozess für die abhängigen Hardware-iSCSI-Adapter besteht aus diesen Schritten:

1 Zeigen Sie die abhängigen Hardware-Adapter an.

   Weitere Informationen hierzu finden Sie unter „Anzeigen abhängiger Hardware-iSCSI-Adapter“, auf Seite 36.

   Falls Ihre abhängigen Hardware-Adapter nicht in der Liste der Speicheradapter angezeigt werden, überprüfen Sie, ob sie lizenziert werden müssen. Informationen finden Sie in der Dokumentation des Anbieters.

2 Ermitteln Sie, welchen physischen Netzwerkkarten die abhängigen Hardware-Adapter zugeordnet sind.

   Weitere Informationen hierzu finden Sie unter „Ermitteln der Zuordnung zwischen abhängigem Hardware-iSCSI und physischem Netzwerkadapter“, auf Seite 36.

   Notieren Sie sich die Namen der zugehörigen physischen Netzwerkkarten. Beispielsweise gehört der Adapter „vmhba33“ zu „vmnic1“ und „vmhba34“ zu „vmnic2“.

3 Konfigurieren Sie das iSCSI-Netzwerk, indem Sie Ports für den iSCSI-Datenverkehr erstellen.

   Weitere Informationen hierzu finden Sie unter „Netzwerkkonfiguration für Software-iSCSI und abhängige Hardware-iSCSI“, auf Seite 39.

   Öffnen Sie für jede Netzwerkkarte einen Port. Erstellen Sie beispielsweise den Port „vmk1“ für die Netzwerkkarte „vmnic1“ und den Port „vmk2“ für „vmnic2“.

4 Binden Sie die iSCSI-Ports an entsprechende abhängige Hardware-iSCSI-Adapter. Dieser Schritt ist unabhängig davon erforderlich, ob mehrere oder nur ein Adapter vorhanden sind.

   Weitere Informationen hierzu finden Sie unter „Binden von iSCSI-Ports an iSCSI-Adapter“, auf Seite 43.

   In diesem Beispiel binden Sie den Port „vmk1“ an „vmhba33“ und den Port „vmk2“ an „vmhba34“.

5 Erkennungsadressen konfigurieren.

   Weitere Informationen hierzu finden Sie unter „Konfigurieren von Erkennungsadressen für iSCSI-Initiatoren“, auf Seite 46.

6 CHAP-Parameter konfigurieren.

   Weitere Informationen hierzu finden Sie unter „Konfigurieren von CHAP-Parametern für iSCSI-Adapter“, auf Seite 48.

Überlegungen zu abhängigen Hardware-iSCSI-Adaptern

Wenn Sie abhängige Hardware-iSCSI-Adapter für ESX/ESXi verwenden, muss Folgendes beachtet werden.

- Wenn Sie einen abhängigen Hardware-iSCSI-Adapter verwenden, zeigt der Leistungsbericht für eine dem Adapter zugewiesene Netzwerkkarte möglicherweise wenig oder keine Aktivität, selbst wenn eine große Menge an iSCSI-Datenverkehr vorhanden ist. Dieses Verhalten tritt auf, weil der iSCSI-Datenverkehr den regulären Netzwerkstack umgeht.
- Der Broadcom iSCSI-Adapter führt eine Datenumwandlung in Hardware mit begrenztem Pufferspeicher durch. Wenn Sie den Broadcom iSCSI-Adapter in einem ausgelasteten oder überlasteten Netzwerk verwenden, aktivieren Sie die Flusssteuerung, damit die Leistung nicht beeinträchtigt wird.

  Die Flusssteuerung überwacht die Datenübertragungsrate zwischen zwei Knoten und verhindert, dass ein langsamer Empfänger von einem schnellen Sender überrannt wird. Um optimale Ergebnisse zu erzielen, aktivieren Sie die Flusssteuerung an den Endpunkten des E/A-Pfads, d. h. auf den Hosts und den iSCSI-Speichersystemen.
- IPv6 und Jumbo-Frames werden von Broadcom iSCSI-Adaptern nicht unterstützt.

Anzeigen abhängiger Hardware-iSCSI-Adapter

Zeigen Sie einen abhängigen Hardware-iSCSI-Adapter an, um zu überprüfen, ob er korrekt geladen ist.

Falls der abhängige Hardware-Adapter nicht in der Liste der Speicheradapter angezeigt wird, überprüfen Sie, ob er lizenziert werden muss. Informationen finden Sie in der Dokumentation des Anbieters.

Vorgehensweise

1 Melden Sie sich am vSphere-Client an und wählen Sie einen Host im Bestandslistenbereich aus.

2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend unter **[Hardware]** auf **[Speicheradapter]** .

  Falls installiert, sollte der abhängige Hardware-iSCSI-Adapter in der Liste der Speicheradapter angezeigt werden.

3 Wählen Sie den Adapter aus, der angezeigt werden soll, und klicken Sie auf **[Eigenschaften]** .

  Das Dialogfeld „iSCSI-Initiator-Eigenschaften“ enthält die standardmäßigen Detailinformationen zu dem Adapter, einschließlich des iSCSI-Namens und des iSCSI-Alias.

Ermitteln der Zuordnung zwischen abhängigem Hardware-iSCSI und physischem Netzwerkadapter

Ermitteln Sie den Namen der physischen Netzwerkkarte, die dem abhängigen Hardware-iSCSI-Adapter zugeordnet ist. Sie müssen die Zuordnung wissen, damit Sie die Port-Bindung ordnungsgemäß durchführen können.

Vorgehensweise

1 Verwenden Sie den vSphere-CLI-Befehl, um den Namen der physischen Netzwerkkarte zu ermitteln, die dem iSCSI-Adapter zugeordnet ist.

  ```
  esxcli swiscsi vmnic list –d vmhba#
  ```

  vmhba# ist der Name des iSCSI-Adapters.

2 Suchen Sie in der Ausgabe folgende Zeile: `vmnic name: vmnic#`.

  vmnic# ist der Name des Netzwerkadapters, der dem iSCSI-Adapter zugeordnet ist.

Weiter

Nachdem Sie den Namen der Netzwerkkarte ermittelt haben, erstellen Sie auf einem vSwitch, der mit der Netzwerkkarte verbunden ist, einen iSCSI-Port. Anschließend binden Sie diesen Port an den abhängigen Hardware-iSCSI-Adapter, sodass Ihr Host den iSCSI-Datenverkehr durch die Netzwerkkarte leiten kann.

Einrichten und Konfigurieren des Software-iSCSI-Adapters

Bei der softwarebasierten iSCSI-Implementierung können Sie Standard-Netzwerkkarten verwenden, um Ihren Host mit einem externen iSCSI-Ziel im IP-Netzwerk zu verbinden. Der in ESX/ESXi integrierte Software-iSCSI-Adapter ermöglicht diese Verbindung, indem er über den Netzwerkstapel mit den physischen Netzwerkkarten kommuniziert.

Wenn Sie über den vSphere-Client eine Verbindung mit dem vCenter Server oder dem Host herstellen, wird der Software-iSCSI-Adapter in der Liste der Speicheradapter angezeigt. Es wird nur ein Software-iSCSI-Adapter angezeigt. Bevor Sie den Software-iSCSI-Adapter verwenden können, müssen Sie ein Netzwerk einrichten, den Adapter aktivieren und Parameter, wie z. B. Erkennungsadressen und CHAP, konfigurieren. Der Workflow zur Konfiguration des Software-iSCSI-Adapters umfasst die folgenden Schritte:

1 Konfigurieren Sie das iSCSI-Netzwerk, indem Sie Ports für den iSCSI-Datenverkehr erstellen.

   Weitere Informationen hierzu finden Sie unter „Netzwerkkonfiguration für Software-iSCSI und abhängige Hardware-iSCSI“, auf Seite 39.

2 Aktivieren Sie den Software-iSCSI-Adapter.

   Weitere Informationen hierzu finden Sie unter „Aktivieren des Software-iSCSI-Adapters“, auf Seite 37.

3 Wenn Sie für das Software-iSCSI-Multipathing mehrere Netzwerkkarten verwenden, führen Sie die Port-Bindung durch, indem Sie alle iSCSI-Ports mit dem Software-iSCSI-Adapter verbinden.

   Weitere Informationen hierzu finden Sie unter „Binden von iSCSI-Ports an iSCSI-Adapter“, auf Seite 43.

4 Aktivieren Sie bei Bedarf Jumbo-Frames. Jumbo-Frames müssen für jeden vSwitch über die vSphere-CLI aktiviert werden.

5 Erkennungsadressen konfigurieren.

   Weitere Informationen hierzu finden Sie unter „Konfigurieren von Erkennungsadressen für iSCSI-Initiatoren“, auf Seite 46.

6 CHAP-Parameter konfigurieren.

   Weitere Informationen hierzu finden Sie unter „Konfigurieren von CHAP-Parametern für iSCSI-Adapter“, auf Seite 48.

Aktivieren des Software-iSCSI-Adapters

Sie müssen Ihren Software-iSCSI-Adapter aktivieren, damit er von Ihrem Host für den Zugriff auf den iSCSI-Speicher verwendet werden kann.

Voraussetzungen

Richten Sie eine Vernetzung für iSCSI ein, bevor Sie den Software-iSCSI-Adapter aktivieren.

HINWEIS Wenn Sie von iSCSI mithilfe des Software-iSCSI-Adapters starten, wird der Adapter aktiviert und die Netzwerkkonfiguration wird automatisch beim ersten Boot-Vorgang erstellt. Wenn Sie den Adapter deaktivieren, wird er bei jedem Neustart des Hosts erneut aktiviert.

Vorgehensweise

1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenbereich auf den Server.

2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend unter **[Hardware]** auf **[Speicheradapter]** .

Ein Verzeichnis der verfügbaren Speicheradapter wird angezeigt.

3 Wählen Sie den zu konfigurierenden iSCSI-Initiator aus und klicken Sie auf **[Eigenschaften]** .

4 Klicken Sie auf **[Konfigurieren]** .

5 Aktivieren Sie das Kontrollkästchen **[Aktiviert]** und klicken Sie auf **[OK]** .

Nachdem Sie den Initiator aktiviert haben, weist ihm der Host den Standard-iSCSI-Namen zu. Sie können den Standardnamen bei Bedarf ändern.

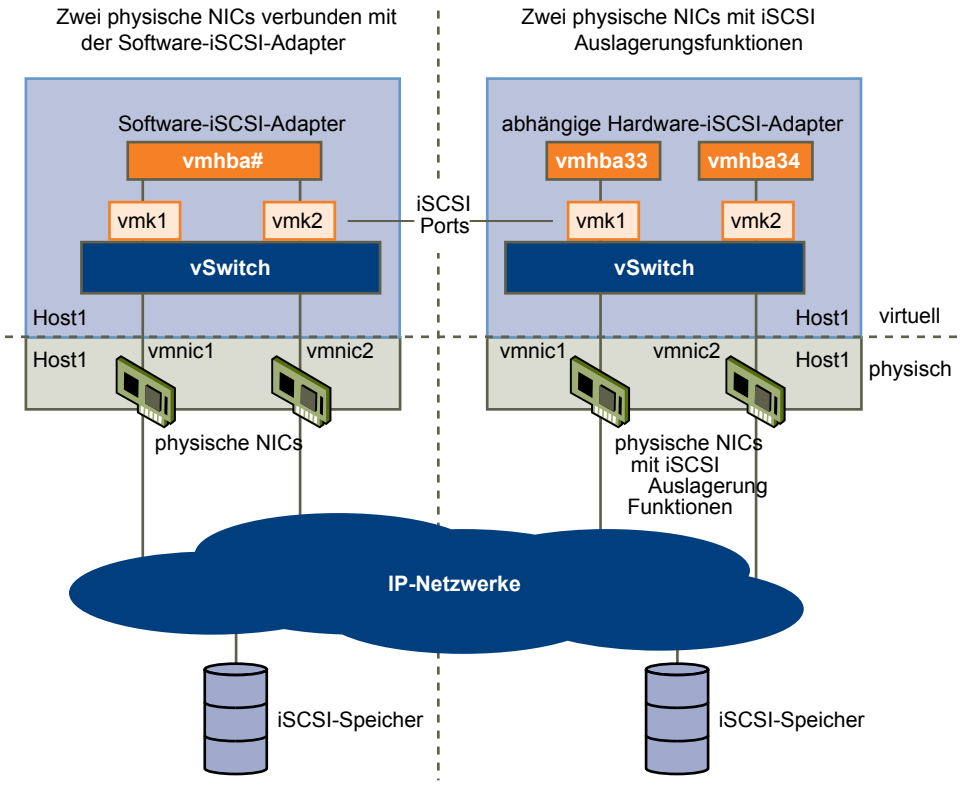
Netzwerkkonfiguration für Software-iSCSI und abhängige Hardware-iSCSI

Wenn Sie den Software-iSCSI-Adapter oder abhängige Hardware-iSCSI-Adapter verwenden, müssen Sie das Netzwerk für iSCSI einrichten, bevor Sie Ihre iSCSI-Adapter aktivieren und konfigurieren können. Die Netzwerkkonfiguration für iSCSI umfasst das Öffnen eines VMkernel-iSCSI-Ports für den Datenverkehr zwischen dem iSCSI-Adapter und der physischen Netzwerkkarte.

Abhängig von der Anzahl an physischen Netzwerkkarten, die Sie für den iSCSI-Datenverkehr verwenden möchten, sind unterschiedliche Netzwerk-Setups möglich.

- Wenn eine einzelne physische Netzwerkkarte vorhanden ist, erstellen Sie einen iSCSI-Port auf einem vSwitch, der mit der Netzwerkkarte verbunden ist. VMware empfiehlt, einen separaten Netzwerkadapter für iSCSI festzulegen. Verwenden Sie iSCSI nicht bei Adaptern mit 100 MBit/s oder weniger.
- Wenn Sie mehrere physische Netzwerkkarten für iSCSI verwenden, erstellen Sie für jede physische Netzwerkkarte einen separaten iSCSI-Port und verwenden Sie die Netzwerkkarten zum iSCSI-Multipathing. Weitere Informationen hierzu finden Sie unter Abbildung 2-1.

Abbildung 2-1. Netzwerk mit iSCSI



Hinweis Wenn Sie einen abhängigen Hardware-iSCSI-Adapter verwenden, zeigt der Leistungsbericht für eine dem Adapter zugewiesene Netzwerkkarte möglicherweise wenig oder keine Aktivität, selbst wenn eine große Menge an iSCSI-Datenverkehr vorhanden ist. Dieses Verhalten tritt auf, weil der iSCSI-Datenverkehr den regulären Netzwerkstack umgeht.

- Erstellen eines iSCSI-Ports für eine einzelne Netzwerkkarte auf Seite 40

  Mit diesem Verfahren können Sie den VMkernel, der Dienste für den iSCSI-Speicher ausführt, an eine physische Netzwerkkarte anschließen. Wenn Sie nur über einen physischen Netzwerkadapter für iSCSI-Datenverkehr verfügen, ist dies das einzige Verfahren, das Sie zum Einrichten Ihres iSCSI-Netzwerks ausführen müssen.

- Verwenden mehrerer Netzwerkkarten für Software-iSCSI und abhängige Hardware-iSCSI auf Seite 40

  Wenn Ihr Host mehrere physische Netzwerkkarten für iSCSI besitzt, erstellen Sie mithilfe einer 1:1-Zuordnung für jede physische Netzwerkkarte einen separaten iSCSI-Port.

- Erstellen zusätzlicher iSCSI-Ports für mehrere Netzwerkkarten auf Seite 41

  Verwenden Sie dieses Verfahren, wenn zwei oder mehr Netzwerkkarten vorhanden sind, die Sie für iSCSI auswählen können, und Sie alle iSCSI-Netzwerkkarten mit einem einzigen vSwitch verbinden möchten. In dieser Aufgabe ordnen Sie VMkernel-iSCSI-Ports mithilfe einer 1:1-Zuordnung den Netzwerkadaptern zu.

Erstellen eines iSCSI-Ports für eine einzelne Netzwerkkarte

Mit diesem Verfahren können Sie den VMkernel, der Dienste für den iSCSI-Speicher ausführt, an eine physische Netzwerkkarte anschließen. Wenn Sie nur über einen physischen Netzwerkadapter für iSCSI-Datenverkehr verfügen, ist dies das einzige Verfahren, das Sie zum Einrichten Ihres iSCSI-Netzwerks ausführen müssen.

Vorgehensweise

1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenbereich auf den Host.

2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Netzwerk]** .

3 Klicken Sie in der Ansicht „Virtueller Switch“ auf **[Netzwerk hinzufügen]** .

4 Wählen Sie **[VMkernel]** aus und klicken Sie auf **[Weiter]** .

5 Wählen Sie **[Einen virtuellen Switch erstellen]** , um einen neuen vSwitch zu erstellen.

6 Wählen Sie eine Netzwerkkarte aus, die Sie für iSCSI-Datenverkehr verwenden möchten.

WICHTIG Wenn Sie einen Port für den abhängigen Hardware-iSCSI-Adapter erstellen, stellen Sie sicher, dass Sie die Netzwerkkarte auswählen, die zu der iSCSI-Komponente gehört. Weitere Informationen hierzu finden Sie unter „Ermitteln der Zuordnung zwischen abhängigem Hardware-iSCSI und physischem Netzwerkadapter“, auf Seite 36.

---

7 Klicken Sie auf **[Weiter]** .

8 Geben Sie eine Netzwerkbezeichnung ein.

Die Netzwerkbezeichnung ist ein aussagekräftiger Name, der den VMkernel-Port identifiziert, den Sie erstellen, z. B. iSCSI.

9 Klicken Sie auf **[Weiter]** .

10 Geben Sie die IP-Einstellungen an und klicken Sie auf **[Weiter]** .

11 Überprüfen Sie die Informationen und klicken Sie auf **[Beenden]** .

Verwenden mehrerer Netzwerkkarten für Software-iSCSI und abhängige Hardware-iSCSI

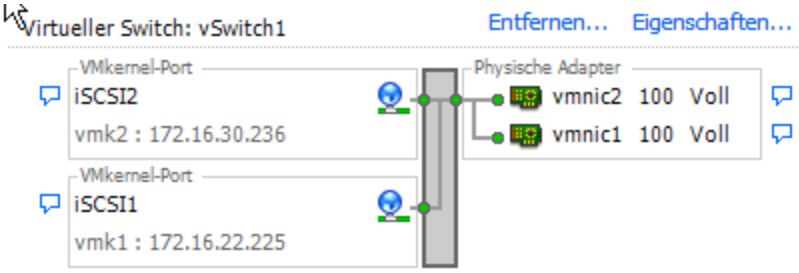
Wenn Ihr Host mehrere physische Netzwerkkarten für iSCSI besitzt, erstellen Sie mithilfe einer 1:1-Zuordnung für jede physische Netzwerkkarte einen separaten iSCSI-Port.

Um eine 1:1-Zuordnung zu erreichen, legen Sie für jedes Paar aus Netzwerkadapter und iSCSI-Port einen separaten vSwitch fest. Weitere Informationen hierzu finden Sie unter Abbildung 2-2.

Abbildung 2-2. iSCSI-Ports und Netzwerkkarten auf separaten vSwitches

Eine Alternative besteht darin, alle Paare aus Netzwerkkarte und iSCSI-Port zu einem einzigen vSwitch hinzuzufügen. Weitere Informationen hierzu finden Sie unter Abbildung 2-3. Sie müssen das Standard-Setup überschreiben und sicherstellen, dass jeder Port lediglich einer entsprechenden aktiven Netzwerkkarte zugeordnet wird.

Abbildung 2-3. iSCSI-Ports und Netzwerkkarten auf einem einzigen vSwitch



Weitere Informationen über das Hinzufügen von Paaren aus Netzwerkkarte und VMkernel-Port finden Sie unter „Erstellen zusätzlicher iSCSI-Ports für mehrere Netzwerkkarten“, auf Seite 41.

Binden Sie nach dem Zuordnen von iSCSI-Ports zu Netzwerkadaptern mithilfe des Befehls `esxcli` die Ports an die iSCSI-Adapter. Führen Sie bei abhängigen Hardware-iSCSI-Adaptern eine Port-Bindung durch, egal, ob Sie eine oder mehrere Netzwerkkarten verwenden. Weitere Informationen hierzu finden Sie unter „Binden von iSCSI-Ports an iSCSI-Adapter“, auf Seite 43.

Erstellen zusätzlicher iSCSI-Ports für mehrere Netzwerkkarten

Verwenden Sie dieses Verfahren, wenn zwei oder mehr Netzwerkkarten vorhanden sind, die Sie für iSCSI auswählen können, und Sie alle iSCSI-Netzwerkkarten mit einem einzigen vSwitch verbinden möchten. In dieser Aufgabe ordnen Sie VMkernel-iSCSI-Ports mithilfe einer 1:1-Zuordnung den Netzwerkadaptern zu.

Jetzt müssen Sie zusätzliche Netzwerkkarten mit dem vorhandenen vSwitch verbinden und sie den entsprechenden iSCSI-Ports zuordnen.

Hinweis Wenn Sie einen verteilten vNetwork-Switch mit mehreren dvUplinks für die Port-Bindung verwenden, erstellen Sie für jede physische Netzwerkkarte eine separate dvPort-Gruppe. Legen Sie anschließend die Teamrichtlinie so fest, dass jede dvPort-Gruppe nur einen aktiven dvUplink besitzt.

Weitere Informationen zu verteilten vNetwork-Switches finden Sie im Abschnitt „Netzwerk“ des *Handbuchs zur Serverkonfiguration für ESX/ESXi*.

Voraussetzungen

Sie müssen einen vSwitch erstellen, der einen iSCSI-Port einer physischen Netzwerkkarte zuordnet, die für den iSCSI-Datenverkehr vorgesehen ist.

Vorgehensweise

1 Melden Sie sich am vSphere-Client an und klicken Sie im Bestandslistenbereich auf den Host.

2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Netzwerk]**.

3 Wählen Sie den vSwitch aus, den Sie für iSCSI verwenden, und klicken Sie auf **[Eigenschaften]**.

4 Verbinden Sie zusätzliche Netzwerkadapter mit dem vSwitch.

   a Klicken Sie im Dialogfeld vSwitch-Eigenschaften auf die Registerkarte **[Netzwerkadapter]** und anschließend auf **[Hinzufügen]** .

   b Wählen Sie mindestens eine Netzwerkkarte in der Liste aus und klicken Sie auf **[Weiter]** .

   Stellen Sie für abhängige Hardware-iSCSI-Adapter sicher, dass Sie nur die Netzwerkkarten auswählen, die eine entsprechende iSCSI-Komponente besitzen.

   c Überprüfen Sie die Informationen auf der Seite Adapterübersicht und klicken Sie auf **[Beenden]** .

   Die Liste der Netzwerkadapter mit den nun dem vSwitch zugewiesenen Netzwerkadaptern wird erneut angezeigt.

5 Erstellen Sie iSCSI-Ports für alle Netzwerkkarten, die Sie verbunden haben.

   Die Anzahl an iSCSI-Ports muss mit der Anzahl an Netzwerkkarten auf dem vSwitch übereinstimmen.

   a Klicken Sie im Dialogfeld „vSwitch-Eigenschaften“ auf die Registerkarte **[Ports]** und anschließend auf **[Hinzufügen]** .

   b Wählen Sie **[VMkernel]** aus und klicken Sie auf **[Weiter]** .

   c Geben Sie unter **[Portgruppeneigenschaften]** eine Netzwerkbezeichnung ein, z. B. „iSCSI“, und klicken Sie auf **[Weiter]** .

   d Geben Sie die IP-Einstellungen an und klicken Sie auf **[Weiter]** .

   Wenn Sie eine Subnetzmaske eingeben, stellen Sie sicher, dass die Netzwerkkarte auf das Subnetz des Speichersystems eingestellt ist, mit dem sie verbunden wird.

   e Überprüfen Sie die Informationen und klicken Sie auf **[Beenden]** .

Vorsicht Wenn sich die Netzwerkkarte, die Sie mit Ihrem Software- oder abhängigen Hardware-iSCSI-Adapter verwenden, nicht im selben Subnetz befindet wie Ihr iSCSI-Ziel, kann Ihr Host keine Sitzungen von diesen Netzwerkadapter zum Ziel einrichten.

6 Ordnen Sie jeden iSCSI-Port nur einer aktiven Netzwerkkarte zu.

   Standardmäßig werden für jeden iSCSI-Port auf dem vSwitch alle Netzwerkadapter als aktiv angezeigt. Sie müssen dieses Setup überschreiben, damit jeder Port lediglich einer aktiven Netzwerkkarte zugeordnet wird. Beispielsweise wird der iSCSI-Port „vmk1“ der Netzwerkkarte „vmnic1“ zugeordnet, der Port „vmk2“ wird „vmnic2“ zugeordnet usw.

   a Wählen Sie auf der Registerkarte **[Ports]** einen iSCSI-Port aus und klicken Sie auf **[Bearbeiten]** .

   b Klicken Sie auf die Registerkarte **[NIC-Gruppierung]** und wählen Sie **[Reihenfolge für vSwitch-Failover außer Kraft setzen]** .

   c Wählen Sie nur einen Adapter als aktiv aus und verschieben Sie alle übrigen Adapter in die Kategorie **[Nicht verwendete Adapter]** .

7 Wiederholen Sie diesen letzten Schritt für jeden iSCSI-Port auf dem vSwitch.

Weiter

Verwenden Sie nach dem Ausführen dieser Aufgabe den Befehl `esxcli`, um die iSCSI-Ports an die Software-iSCSI- oder abhängigen Hardware-iSCSI-Adapter zu binden.

Binden von iSCSI-Ports an iSCSI-Adapter

Binden Sie einen iSCSI-Port, den Sie für eine Netzwerkkarte erstellt haben, an einen iSCSI-Adapter. Führen Sie diese Aufgabe für den Software-iSCSI-Adapter nur dann aus, wenn Sie mindestens zwei Netzwerkkarten für das iSCSI-Multipathing einrichten. Wenn Sie abhängige Hardware-iSCSI-Adapter verwenden, muss die Aufgabe unabhängig davon, ob mehrere oder nur ein Adapter vorhanden sind, ausgeführt werden.

Voraussetzungen

Führen Sie die folgenden Aufgaben aus:

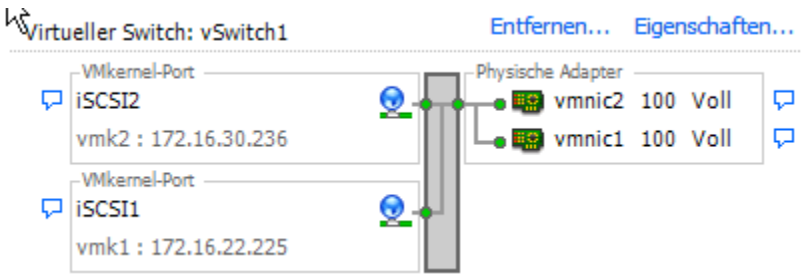
- Stellen Sie für abhängige Hardware-iSCSI-Adapter sicher, dass die Verbindung zwischen den physischen Netzwerkkarten und den iSCSI-Adaptern korrekt ist. Weitere Informationen hierzu finden Sie unter „Anzeigen abhängiger Hardware-iSCSI-Adapter“, auf Seite 36.
- Richten Sie die Vernetzung für den iSCSI-Datenverkehr ein. Weitere Informationen hierzu finden Sie unter „Netzwerkkonfiguration für Software-iSCSI und abhängige Hardware-iSCSI“, auf Seite 39.
- Aktivieren Sie den Software-iSCSI-Adapter, um ihn verwenden zu können. Weitere Informationen hierzu finden Sie unter „Aktivieren des Software-iSCSI-Adapters“, auf Seite 37.

Vorgehensweise

1 Identifizieren Sie den Namen des iSCSI-Ports, der der physischen Netzwerkkarte zugewiesen ist.

Der vSphere-Client zeigt den Portnamen unter der Netzwerkbezeichnung an.

In der nachfolgenden Abbildung haben die Ports die Namen „vmk1“ und „vmk2“.



2 Verwenden Sie den vSphere-CLI-Befehl, um den iSCSI-Port an den iSCSI-Adapter zu binden.

```
esxcli swiscsi nic add –n Portname –d vmhba
```

WICHTIG Wiederholen Sie für Software-iSCSI diesen Befehl für jeden iSCSI-Port, sodass alle Ports mit dem Software-iSCSI-Adapter verbunden werden. Stellen Sie für abhängige Hardware-iSCSI sicher, dass jeder Port an einen entsprechenden, geeigneten Adapter gebunden wird.

3 Überprüfen Sie, ob der Port zum iSCSI-Adapter hinzugefügt wurde.

```
esxcli swiscsi nic list –d vmhba
```

4 Prüfen Sie den iSCSI-Adapter mithilfe des vSphere-Clients neu.

Binden von iSCSI-Ports an iSCSI-Adapter

Lesen Sie die Beispiele zum Binden mehrerer Ports, die Sie für physische Netzwerkkarten erstellt haben, an den Software-iSCSI-Adapter oder an mehreren abhängigen Hardware-iSCSI-Adaptern.

Beispiel 2-1. Verbinden von iSCSI-Ports mit dem Software-iSCSI-Adapter

Dieses Beispiel zeigt, wie Sie die iSCSI-Ports „vmk1“ und „vmk2“ mit dem Software-iSCSI-Adapter „vmhba33“ verbinden.

1 Verbinden Sie „vmk1“ mit „vmhba33“: **`esxcli swiscsi nic add –n vmk1 –d vmhba33`**.

2 Verbinden Sie „vmk2“ mit „vmhba33“: **`esxcli swiscsi nic add –n vmk2 –d vmhba33`**.

3 Verifizieren Sie die Konfiguration von „vmhba33“: **`esxcli swiscsi nic list –d vmhba33`**.

Sowohl „vmk1“ als auch „vmk2“ sollten aufgelistet sein.

Wenn Sie über den vSphere-Client die Pfadansicht für den Adapter „vmhba33“ anzeigen, sehen Sie, dass der Adapter zwei Pfade für den Zugriff auf dasselbe Ziel verwendet. Die Laufzeitnamen der Pfade lauten „vmhba33:C1:T1:L0“ und „vmhba33:C2:T1:L0“. In diesem Beispiel geben „C1“ und „C2“ die beiden Netzwerkadapter an, die für das Multipathing verwendet werden.

Beispiel 2-2. Verbinden von iSCSI-Ports mit abhängigen Hardware-iSCSI-Adaptern

Dieses Beispiel zeigt, wie Sie die iSCSI-Ports „vmk1“ und „vmk2“ mit den entsprechenden Hardware-iSCSI-Adaptern „vmhba33“ und „vmhba34“ verbinden.

1 Verbinden Sie „vmk1“ mit „vmhba33“: **`esxcli swiscsi nic add –n vmk1 –d vmhba33`**.

2 Verbinden Sie „vmk2“ mit „vmhba34“: **`esxcli swiscsi nic add –n vmk2 –d vmhba34`**.

3 Verifizieren Sie die Konfiguration von „vmhba33“: **`esxcli swiscsi nic list –d vmhba33`**.

4 Verifizieren Sie die Konfiguration von „vmhba34“: **`esxcli swiscsi nic list –d vmhba34`**.

Trennen der iSCSI-Ports von iSCSI-Adaptern

Falls Sie Änderungen an der Netzwerkkonfiguration vornehmen müssen, die Sie für den iSCSI-Datenverkehr verwenden, um beispielsweise eine Netzwerkkarte oder einen iSCSI-Port zu entfernen, stellen Sie sicher, dass Sie den iSCSI-Port vom iSCSI-Adapter getrennt haben.

Wichtig Falls aktive iSCSI-Sitzungen zwischen Ihrem Host und den Zielen bestehen, können Sie die Verbindung des iSCSI-Ports trennen.

Vorgehensweise

1 Verwenden Sie die vSphere-CLI, um die Verbindung des iSCSI-Ports mit dem iSCSI-Adapter zu trennen.

`esxcli swiscsi nic remove –n` ***`Portname`*** **`–d`** ***`vmhba`***

2 Überprüfen Sie, ob die Verbindung des Ports zum iSCSI-Adapter getrennt wurde.

`esxcli swiscsi nic list –d` ***`vmhba`***

3 Prüfen Sie den iSCSI-Adapter mithilfe des vSphere-Clients neu.

Verwenden von Jumbo-Frames mit iSCSI

Mithilfe von Jumbo-Frames kann ESX/ESXi größere Frames an das physische Netzwerk senden. Das Netzwerk muss Jumbo-Frames durchgängig unterstützen, damit diese Technologie eingesetzt werden kann. Jumbo-Frames bis zu 9 KB (9000 Byte) werden unterstützt.

Tabelle 2-1 erläutert den Umfang der Unterstützung, die ESX/ESXi für Jumbo-Frames bereitstellt.

Tabelle 2-1. Unterstützung für Jumbo-Frames

Typ des iSCSI-Adapters	Unterstützung für Jumbo-Frames	Kommentar
Software-iSCSI	Unterstützt	Informieren Sie sich bei Ihrem Anbieter, ob Ihr physischer Netzwerkadapter und Ihr iSCSI-Speicher Jumbo-Frames unterstützen.
Abhängige Hardware-iSCSI	Unterstützt	Broadcom-abhängige iSCSI-Adapter unterstützen Jumbo-Frames nicht.
Unabhängige Hardware-iSCSI	Nicht unterstützt	

Aktivieren von Jumbo-Frames für Software-iSCSI und abhängige Hardware-iSCSI

Verwenden Sie die vSphere-CLI, um Jumbo-Frames für jeden vSwitch zu aktivieren, der für den iSCSI-Datenverkehr ausgewählt ist. Außerdem müssen Sie eine für Jumbo-Frames aktivierte VMkernel-Netzwerkschnittstelle erstellen.

1 Aktivieren von Jumbo-Frames auf einem vSwitch auf Seite 45

   Ändern Sie zum Aktivieren von Jumbo-Frames auf einem vSwitch die MTU-Konfiguration für den entsprechenden vSwitch.

2 Erstellen einer für Jumbo-Frames aktivierten VMkernel-Schnittstelle auf Seite 46

   Verwenden Sie die vSphere-CLI, um eine für Jumbo-Frames aktivierte VMkernel-Netzwerkschnittstelle zu erstellen.

Aktivieren von Jumbo-Frames auf einem vSwitch

Ändern Sie zum Aktivieren von Jumbo-Frames auf einem vSwitch die MTU-Konfiguration für den entsprechenden vSwitch.

Vorgehensweise

1 Führen Sie über die vSphere-CLI den Befehl **`vicfg-vswitch -m MTU`** ***`vSwitch`*** aus.

   Dieser Befehl legt die MTU für alle physischen Netzwerkkarten auf diesem vSwitch fest. Legen Sie als MTU-Größe die größte MTU-Größe von allen Netzwerkkarten fest, die mit dem vSwitch verbunden sind.

2 Führen Sie den Befehl **`vicfg-vswitch -l`** aus, um eine Liste der vSwitches auf dem Host anzuzeigen, und prüfen Sie, ob die Konfiguration des vSwitches ordnungsgemäß ist.

Erstellen einer für Jumbo-Frames aktivierten VMkernel-Schnittstelle

Verwenden Sie die vSphere-CLI, um eine für Jumbo-Frames aktivierte VMkernel-Netzwerkschnittstelle zu erstellen.

Vorgehensweise

1 Geben Sie in der vSphere-CLI den Befehl `vicfg–vmknic` ein, um eine VMkernel-Verbindung mit Jumbo-Frame-Unterstützung herzustellen.

```
vicfg–vmknic –a –I IP–Adresse –n Netzmaske –m MTU Name der Portgruppe
```

2 Führen Sie den Befehl `vicfg–vmknic –l` aus, um eine Liste der VMkernel-Schnittstellen anzuzeigen, und prüfen Sie, ob die Konfiguration der für Jumbo-Frames aktivierten Schnittstelle korrekt ist.

3 Stellen Sie sicher, dass die VMkernel-Schnittstelle mit einem für Jumbo Frames aktivierten vSwitch verbunden ist.

4 Konfigurieren Sie alle physischen Switches sowie alle physischen oder virtuellen Maschinen für die Unterstützung von Jumbo Frames, mit denen diese VMkernel-Schnittstelle eine Verbindung herstellt.

Konfigurieren von Erkennungsadressen für iSCSI-Initiatoren

Sie müssen Zielerkennungsadressen einrichten, damit der iSCSI-Initiator erkennen kann, welche Speicherressourcen im Netzwerk zur Verfügung stehen.

Das ESX/ESXi-System unterstützt die folgenden Erkennungsmethoden:

Dynamische Erkennung Wird auch als „SendTargets“-Erkennung bezeichnet. Immer wenn der Initiator einen angegebenen iSCSI-Server kontaktiert, übermittelt der Initiator eine „SendTargets“-Anforderung an den Server. Der Server liefert als Antwort eine Liste verfügbarer Ziele an den Initiator zurück. Die Namen und IP-Adressen dieser Ziele werden auf der Registerkarte **[Statische Erkennung (Static Discovery)]** angezeigt. Wenn Sie ein von der dynamischen Erkennung hinzugefügtes statisches Ziel entfernen, kann das Ziel entweder bei einer erneuten Überprüfung, beim Zurücksetzen des HBA oder durch einen Neustart des Hosts erneut zur Liste hinzugefügt werden.

Statische Erkennung Der Initiator muss keine Erkennung durchführen. Der Initiator kennt bereits alle Ziele, mit denen er Kontakt aufnehmen möchte, und verwendet ihre IP-Adressen und Domänennamen für die Kommunikation mit ihnen.

Einrichten der dynamischen Erkennung

Mit der dynamischen Erkennung wird jedes Mal, wenn der Initiator einen angegebenen iSCSI-Server kontaktiert, eine „SendTargets“-Anforderung an den Server übermittelt. Der Server liefert als Antwort eine Liste verfügbarer Ziele an den Initiator zurück.

Wenn Sie die dynamische Erkennung einrichten, können Sie nur einen neuen iSCSI-Server hinzufügen. Sie können die IP-Adresse, den DNS-Namen oder die Portnummer eines vorhandenen iSCSI-Servers nicht ändern. Wenn Sie Änderungen vornehmen möchten, entfernen Sie den vorhandene Server und fügen Sie einen neuen hinzu.

Vorgehensweise

1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend unter **[Hardware]** auf **[Speicheradapter]** .

Ein Verzeichnis der verfügbaren Speicheradapter wird angezeigt.

3 Wählen Sie den zu konfigurierenden iSCSI-Initiator aus und klicken Sie auf **[Eigenschaften]** .

4 Klicken Sie im Dialogfeld **[iSCSI-Initiator-Eigenschaften]** auf die Registerkarte **[Dynamische Erkennung]** .

5 Um der „SendTargets“-Erkennungsmethode eine Adresse hinzuzufügen, klicken Sie auf **[Hinzufügen]** .

Daraufhin wird das Dialogfeld **['SendTarget'-Server hinzufügen]** angezeigt.

6 Geben Sie die IP-Adresse oder den DNS-Namen des Speichersystems ein und klicken Sie auf **[OK]** .

Nachdem der Host die „SendTargets“-Sitzung mit diesem System gestartet hat, werden in der Liste „Statische Erkennung“ alle neu erkannten Ziele angezeigt.

7 Sie können einen bestimmten „SendTargets“-Server löschen, indem Sie ihn auswählen und auf **[Entfernen]** klicken.

Nachdem Sie einen „SendTargets“-Server entfernt haben, wird er möglicherweise immer noch im Feld „Vererbung“ als übergeordnetes Element von statischen Zielen angezeigt. Dieser Eintrag zeigt an, wo die statischen Ziele ermittelt wurden, und wirkt sich nicht auf die Funktionsweise aus.

Weiter

Nachdem Sie die dynamische Erkennung für Ihren iSCSI-Adapter eingerichtet haben, prüfen Sie den Adapter erneut.

Einrichten der statischen Erkennung

Bei iSCSI-Initiatoren können Sie neben der dynamischen Erkennungsmethode auch die statische Erkennung verwenden und Informationen für die Ziele manuell eingeben.

Wenn Sie die statische Erkennung einrichten, können Sie nur iSCSI-Ziele hinzufügen. Sie können die IP-Adresse, den DNS-Namen, den iSCSI-Zielnamen oder die Portnummer eines vorhandenen Ziels nicht ändern. Wenn Sie Änderungen vornehmen möchten, entfernen Sie das vorhandene Ziel und fügen Sie ein neues hinzu.

Vorgehensweise

1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend unter **[Hardware]** auf **[Speicheradapter]** .

Ein Verzeichnis der verfügbaren Speicheradapter wird angezeigt.

3 Wählen Sie den zu konfigurierenden iSCSI-Initiator aus und klicken Sie auf **[Eigenschaften]** .

4 Klicken Sie im Dialogfeld **[iSCSI-Initiator-Eigenschaften]** auf die Registerkarte **[Statische Erkennung (Static Discovery)]** .

Die Registerkarte zeigt alle dynamisch erkannten Ziele und alle bereits eingegebenen statischen Ziele an.

5 Um ein Ziel hinzuzufügen, klicken Sie auf **[Hinzufügen]** und geben Sie die Informationen des Ziels ein.

6 Sie können ein bestimmtes Ziel löschen, indem Sie das Ziel auswählen und auf **[Entfernen]** klicken.

Weiter

Nachdem Sie die statische Erkennung für Ihren iSCSI-Adapter eingerichtet haben, prüfen Sie den Adapter erneut.

Konfigurieren von CHAP-Parametern für iSCSI-Adapter

Da die IP-Netzwerke, die die iSCSI-Technologie zum Verbinden mit Remotezielen verwendet, die von ihnen übertragenen Daten nicht schützen, muss die Sicherheit der Verbindung gewährleistet werden. Eines der von iSCSI implementierten Protokolle ist das CHAP (Challenge Handshake Authentication Protocol), das die jeweiligen Berechtigungen der Initiatoren, die auf Ziele im Netzwerk zugreifen, überprüft.

CHAP verwendet einen dreiteiligen Handshake-Algorithmus, um die Identität Ihres Hosts und, sofern zutreffend, des iSCSI-Ziels zu verifizieren, wenn der Host und das Ziel eine Verbindung herstellen. Die Verifizierung basiert auf einem vordefinierten privaten Wert, dem CHAP-Schlüssel, den der Initiator und das Ziel gemeinsam verwenden.

ESX/ESXi unterstützt die CHAP-Authentifizierung auf der Adapterebene. In diesem Fall erhalten alle Ziele vom iSCSI-Initiator denselben CHAP-Namen und -Schlüssel. Für Software- und abhängige Hardware-iSCSI-Adapter unterstützt ESX/ESXi auch die zielbasierte CHAP-Authentifizierung, die Ihnen ermöglicht, unterschiedliche Anmeldedaten für die einzelnen Ziele zu konfigurieren und so die Sicherheit zu erhöhen.

Auswählen der CHAP-Authentifizierungsmethode

ESX/ESXi unterstützt unidirektionales CHAP für alle Typen von iSCSI-Initiatoren und beiderseitiges CHAP für Software- und abhängige Hardware-iSCSI.

Bevor Sie CHAP konfigurieren, überprüfen Sie, ob CHAP im iSCSI-Speichersystem aktiviert ist und welche CHAP-Authentifizierungsmethode vom System unterstützt wird. Wenn CHAP aktiviert ist, müssen Sie es für Ihre Initiatoren aktivieren und dabei sicherstellen, dass die Anmeldedaten für die CHAP-Authentifizierung mit den Anmeldedaten im iSCSI-Speicher übereinstimmen.

ESX/ESXi unterstützt die folgenden CHAP-Authentifizierungsmethoden:

Unidirektionales CHAP Bei der unidirektionalen CHAP-Authentifizierung authentifiziert das Ziel den Initiator, nicht jedoch der Initiator das Ziel.

Beiderseitiges CHAP Bei der beiderseitigen oder bidirektionalen CHAP-Authentifizierung ermöglicht eine zusätzliche Sicherheitsstufe dem Initiator die Authentifizierung des Ziels. VMware unterstützt diese Methode nur für Software- und abhängige Hardware-iSCSI-Adapter.

Für Software- und abhängige Hardware-iSCSI-Adapter können Sie unidirektionales und beiderseitiges CHAP für die einzelnen Initiatoren oder auf der Zielebene festlegen. Hardware-iSCSI unterstützt CHAP nur auf der Initiatorebene.

Wenn Sie die CHAP-Parameter festlegen, geben Sie eine Sicherheitsstufe für CHAP an.

HINWEIS Wenn Sie die CHAP-Sicherheitsebene angeben, ist die Reaktion des Speicher-Arrays anbieterspezifisch und hängt von der CHAP-Implementierung des Arrays ab. Wenn Sie beispielsweise `CHAP verwenden, es sei denn, das Ziel verbietet dies` wählen, verwenden einige Speicher-Arrays CHAP als Reaktion, wobei andere dies nicht tun. Weitere Informationen über das Verhalten der CHAP-Authentifizierung in verschiedenen Initiator- und Zielkonfigurationen finden Sie in der Array-Dokumentation.

Tabelle 2-2. CHAP-Sicherheitsstufe

CHAP-Sicherheitsstufe	Beschreibung	Unterstützt
CHAP nicht verwenden	Der Host verwendet keine CHAP-Authentifizierung. Wählen Sie diese Option aus, um die Authentifizierung zu deaktivieren, wenn sie derzeit aktiviert ist.	Software-iSCSI Abhängige Hardware-iSCSI Unabhängige Hardware-iSCSI
CHAP nur verwenden, wenn Ziel dies erfordert	Der Host bevorzugt eine Nicht-CHAP-Verbindung, er kann jedoch eine CHAP-Verbindung verwenden, wenn das Ziel dies erfordert.	Software-iSCSI Abhängige Hardware-iSCSI
CHAP verwenden, sofern Ziel dies unterstützt	Der Host bevorzugt CHAP, er kann jedoch Nicht-CHAP-Verbindungen verwenden, wenn das Ziel CHAP nicht unterstützt.	Software-iSCSI Abhängige Hardware-iSCSI Unabhängige Hardware-iSCSI
CHAP verwenden	Für den Host ist eine erfolgreiche CHAP-Authentifizierung erforderlich. Die Verbindung schlägt fehl, wenn die CHAP-Aushandlung fehlschlägt.	Software-iSCSI Abhängige Hardware-iSCSI

Einrichten von CHAP-Anmeldedaten für einen iSCSI-Initiator

Alle Ziele können so eingerichtet werden, dass sie denselben CHAP-Namen und -Schlüssel vom iSCSI-Initiator auf der Initiatorebene empfangen. Standardmäßig übernehmen alle Erkennungsadressen und statischen Ziele die CHAP-Parameter, die Sie auf der Initiatorebene einrichten.

Voraussetzungen

Legen Sie vor dem Einrichten von CHAP-Parametern für Software-iSCSI oder abhängige Hardware-iSCSI fest, ob unidirektionales oder beiderseitiges CHAP konfiguriert werden soll. Abhängige Hardware-iSCSI-Adapter unterstützen das beiderseitige CHAP nicht.

- Bei unidirektionalem CHAP authentifiziert das Ziel den Initiator.
- Bei beiderseitigem CHAP authentifizieren sich das Ziel und der Initiator gegenseitig. Stellen Sie sicher, dass Sie für CHAP und beiderseitiges CHAP verschiedene Schlüssel verwenden.

Stellen Sie beim Konfigurieren von CHAP-Parametern sicher, dass sie mit den Parametern auf der Speicherseite übereinstimmen.

Der CHAP-Name darf nicht mehr als 511 und der CHAP-Schlüssel nicht mehr als 255 alphanumerische Zeichen umfassen. Einige Adapter, z. B. der QLogic-Adapter, haben möglicherweise niedrigere Grenzen: 255 für den CHAP-Namen und 100 für den CHAP-Schlüssel.

Vorgehensweise

1 Greifen Sie auf das Dialogfeld „Eigenschaften des iSCSI-Initiators“ zu.

2 Klicken Sie auf der Registerkarte **[Allgemein]** auf **[CHAP]** .

3 Wenn Sie das unidirektionale CHAP konfigurieren möchten, geben Sie unter CHAP Folgendes an:

   a Wählen Sie die CHAP-Sicherheitsstufe.

      - **[CHAP nicht verwenden, sofern nicht vom Ziel benötigt]** (nur Software- und abhängige Hardware-iSCSI)
      - **[CHAP verwenden, sofern Ziel dies unterstützt]**
      - **[CHAP verwenden]** (nur Software- und abhängige Hardware-iSCSI). Um beiderseitiges CHAP konfigurieren zu können, müssen Sie diese Option auswählen.

   b Geben Sie den CHAP-Namen an.

      Stellen Sie sicher, dass der Name, den Sie angeben, mit dem auf der Speicherseite konfigurierten Namen übereinstimmt.

      - Wenn der CHAP-Name dem iSCSI-Initiatornamen entsprechen soll, aktivieren Sie das Kontrollkästchen **[Initiator-Name verwenden]** .
      - Wenn Sie den iSCSI-Initiatornamen nicht als CHAP-Namen verwenden möchten, deaktivieren Sie **[Initiator-Name verwenden]** und geben Sie einen Namen in das Feld **[Name]** ein.

   c Geben Sie einen Schlüssel für unidirektionales CHAP ein, der als Teil der Authentifizierung verwendet werden soll. Stellen Sie sicher, dass Sie denselben Schlüssel verwenden, den Sie auf der Speicherseite eingeben.

4 Wenn Sie beiderseitiges CHAP konfigurieren möchten, konfigurieren Sie zunächst unidirektionales CHAP, indem Sie die Anweisungen unter Schritt 3 befolgen.

   Stellen Sie sicher, dass Sie als Option für unidirektionales CHAP **[CHAP verwenden]** auswählen. Geben Sie anschließend unter **[Beiderseitiges CHAP]** Folgendes an:

   a Wählen Sie die Option **[CHAP verwenden]** aus.

   b Geben Sie den Namen für beiderseitiges CHAP an.

   c Geben Sie den Schlüssel für beiderseitiges CHAP an. Stellen Sie sicher, dass Sie für unidirektionales CHAP und beiderseitiges CHAP verschiedene Schlüssel verwenden.

5 Klicken Sie auf **[OK]** .

6 Prüfen Sie den Initiator erneut.

Wenn Sie die Parameter für CHAP oder beiderseitiges CHAP ändern, werden die neuen Parameter für neue iSCSI-Sitzungen verwendet. Für bestehende Sitzungen werden die neuen Einstellungen erst nach der Ab- und erneuten Anmeldung verwendet.

Einrichten von CHAP-Anmeldedaten für ein Ziel

Für Software- und abhängige Hardware-iSCSI-Adapter können Sie verschiedene CHAP-Anmeldedaten für einzelne Erkennungsadressen oder statische Ziele konfigurieren.

Stellen Sie beim Konfigurieren von CHAP-Parametern sicher, dass sie mit den Parametern auf der Speicherseite übereinstimmen. Der CHAP-Name darf nicht mehr als 511 und der CHAP-Schlüssel nicht mehr als 255 alphanumerische Zeichen umfassen.

Voraussetzungen

Legen Sie vor dem Einrichten von CHAP-Parametern für Software-iSCSI und abhängige Hardware-iSCSI fest, ob unidirektionales oder beiderseitiges CHAP konfiguriert werden soll.

- Bei unidirektionalem CHAP authentifiziert das Ziel den Initiator.
- Bei beiderseitigem CHAP authentifizieren sich das Ziel und der Initiator gegenseitig. Stellen Sie sicher, dass Sie für CHAP und beiderseitiges CHAP verschiedene Schlüssel verwenden.

Vorgehensweise

1 Greifen Sie auf das Dialogfeld „Eigenschaften des iSCSI-Initiators“ zu.

2 Wählen Sie die Registerkarte **[Dynamische Erkennung]** oder **[Statische Erkennung]** aus.

3 Wählen Sie in der Liste der verfügbaren Ziele ein Ziel aus, das Sie konfigurieren möchten, und klicken Sie auf **[Einstellungen] > [CHAP]** .

4 Konfigurieren Sie unidirektionales CHAP im Bereich „CHAP“.

   a Deaktivieren Sie **[Vom übergeordneten Element übernehmen]** .

   b Wählen Sie eine der folgenden Optionen aus:

   - **[CHAP nur verwenden, wenn Ziel dies erfordert]**
   - **[CHAP verwenden, sofern Ziel dies unterstützt]**
   - **[CHAP verwenden]** . Um beiderseitiges CHAP konfigurieren zu können, müssen Sie diese Option auswählen.

   c Geben Sie den CHAP-Namen an.

   Stellen Sie sicher, dass der Name, den Sie angeben, mit dem auf der Speicherseite konfigurierten Namen übereinstimmt.

   - Wenn der CHAP-Name dem iSCSI-Initiatornamen entsprechen soll, aktivieren Sie das Kontrollkästchen **[Initiator-Name verwenden]** .
   - Wenn Sie den iSCSI-Initiatornamen nicht als CHAP-Namen verwenden möchten, deaktivieren Sie **[Initiator-Name verwenden]** und geben Sie einen Namen in das Feld **[Name]** ein.

   d Geben Sie einen Schlüssel für unidirektionales CHAP ein, der als Teil der Authentifizierung verwendet werden soll. Stellen Sie sicher, dass Sie denselben Schlüssel verwenden, den Sie auf der Speicherseite eingeben.

5 Wenn Sie beiderseitiges CHAP konfigurieren möchten, konfigurieren Sie zunächst unidirektionales CHAP, indem Sie die Anweisungen unter Schritt 4 befolgen.

   Stellen Sie sicher, dass Sie als Option für unidirektionales CHAP **[CHAP verwenden]** auswählen. Geben Sie anschließend im Bereich „Beiderseitiges CHAP“ Folgendes an:

   a Deaktivieren Sie **[Vom übergeordneten Element übernehmen]** .

   b Wählen Sie die Option **[CHAP verwenden]** aus.

   c Geben Sie den Namen für beiderseitiges CHAP an.

   d Geben Sie den Schlüssel für beiderseitiges CHAP an. Stellen Sie sicher, dass Sie für unidirektionales CHAP und beiderseitiges CHAP verschiedene Schlüssel verwenden.

6 Klicken Sie auf **[OK]** .

7 Prüfen Sie den Initiator erneut.

Wenn Sie die Parameter für CHAP oder beiderseitiges CHAP ändern, werden die neuen Parameter für neue iSCSI-Sitzungen verwendet. Für bestehende Sitzungen werden die neuen Einstellungen erst nach der Ab- und erneuten Anmeldung verwendet.

Deaktivieren von CHAP

Sie können CHAP deaktivieren, wenn Ihr Speichersystem dieses nicht erfordert.

Wenn Sie CHAP auf einem System deaktivieren, das die CHAP-Authentifizierung benötigt, bleiben bestehende iSCSI-Sitzungen so lange aktiv, bis Sie Ihren ESX/ESXi-Host neu starten oder das Speichersystem eine Abmeldung erzwingt. Nachdem die Sitzung beendet wurde, können Sie keine Verbindungen mehr zu Zielen herstellen, die CHAP benötigen.

Vorgehensweise

1 Öffnen Sie das Dialogfeld „CHAP-Anmeldedaten“.

2 Wenn Sie für Software- und abhängige Hardware-iSCSI-Adapter nur das beiderseitige CHAP deaktivieren, das unidirektionale CHAP jedoch beibehalten möchten, wählen Sie im Bereich „Beiderseitiges CHAP“ **[CHAP nicht verwenden]** aus.

3 Wenn Sie das unidirektionale CHAP deaktivieren möchten, wählen Sie unter CHAP die Option **[CHAP nicht verwenden]** .

   Wenn Sie das unidirektionale CHAP deaktivieren, wird für das beiderseitige CHAP, sofern dies eingerichtet ist, automatisch die Option **[CHAP nicht verwenden]** festgelegt.

4 Klicken Sie auf **[OK]** .

Konfigurieren zusätzlicher Parameter für iSCSI

Möglicherweise müssen Sie für Ihre iSCSI-Initiatoren zusätzliche Parameter konfigurieren. Beispielsweise erfordern einige iSCSI-Speichersysteme eine ARP-Umleitung (Address Resolution Protocol), um iSCSI-Datenverkehr dynamisch von einem Port auf einen anderen zu verschieben. In diesem Fall müssen Sie die ARP-Umleitung auf Ihrem Host aktivieren.

Tabelle 2-3 sind die erweiterten iSCSI-Parameter aufgelistet, die Sie mithilfe des vSphere-Clients konfigurieren können. Darüber hinaus können Sie den vSphere CLI-Befehl `vicfg-iscsi` verwenden, um einige der erweiterten Parameter zu konfigurieren. Weitere Informationen hierzu finden Sie in den Handbüchern *vSphere Command-Line Interface Installation and Scripting Guide und vSphere Command-Line Interface Reference*.

Sie sollten die erweiterten iSCSI-Einstellungen nur ändern, wenn Sie eng mit dem Support-Team von VMware zusammenarbeiten oder anderweitig über umfassende Informationen zu den Werten der einzelnen Einstellungen verfügen.

Tabelle 2-3. Zusätzliche Parameter für iSCSI-Initiatoren

Erweiterte Parameter	Beschreibung	Konfigurierbar auf
Header-Digest	Erhöht die Datenintegrität. Wenn der Parameter „Header-Digest“ aktiviert ist, berechnet das System für den Header-Teil jeder iSCSI-PDU (Protocol Data Unit) eine Prüfsumme und führt anhand des CRC32C-Algorithmus eine Verifizierung durch.	Software-iSCSI Abhängige Hardware-iSCSI
Data Digest	Erhöht die Datenintegrität. Wenn der Parameter „Data Digest“ aktiviert ist, berechnet das System für den Data-Teil jeder PDU eine Prüfsumme und führt anhand des CRC32C-Algorithmus eine Verifizierung durch. **Hinweis** Systeme, die Intel Nehalem-Prozessoren einsetzen, lagern die iSCSI Digest-Berechnungen für Software-iSCSI aus und reduzieren damit die Auswirkungen auf die Leistung.	Software-iSCSI Abhängige Hardware-iSCSI
Maximal ausstehendes R2T	Legt fest, wie viele R2T-PDUs (Ready to Transfer) sich im Übergang befinden können, bevor eine bestätigte PDU empfangen wird.	Software-iSCSI Abhängige Hardware-iSCSI

Tabelle 2-3. Zusätzliche Parameter für iSCSI-Initiatoren (Fortsetzung)

Erweiterte Parameter	Beschreibung	Konfigurierbar auf
Erste Burstlänge	Legt die maximale Menge an nicht angeforderten Daten in Byte fest, die ein iSCSI-Initiator während der Ausführung eines einzelnen SCSI-Befehls an das Ziel senden kann.	Software-iSCSI Abhängige Hardware-iSCSI
Maximale Burstlänge	Die maximale SCSI-Datenlast in einer Data-In- oder einer angeforderten Data-Out-iSCSI-Sequenz in Byte.	Software-iSCSI Abhängige Hardware-iSCSI
Maximale Datensegmentlänge	Die maximale Datensegmentlänge in Byte, die in einer iSCSI-PDU empfangen werden kann.	Software-iSCSI Unabhängige Hardware-iSCSI
Zeitüberschreitung bei der Sitzungswiederherstellung	Gibt den Zeitraum in Sekunden an, der vergehen kann, bevor eine Sitzung wiederhergestellt werden kann. Wird der angegebene Zeitraum überschritten, beendet der iSCSI-Initiator die Sitzung.	Software-iSCSI Abhängige Hardware-iSCSI
No-Op-Intervall	Gibt das Zeitintervall in Sekunden an, in dem NOP-Out-Anforderungen von Ihrem iSCSI-Initiator an ein iSCSI-Ziel gesendet werden. Mithilfe der NOP-Out-Anforderungen kann verifiziert werden, ob zwischen dem iSCSI-Initiator und dem iSCSI-Ziel eine aktive Verbindung besteht.	Software-iSCSI Abhängige Hardware-iSCSI
No-Op-Zeitüberschreitung	Gibt den Zeitraum in Sekunden an, der vergehen kann, bevor Ihr Host eine NOP-In-Meldung erhält. Die Meldung wird vom iSCSI-Ziel als Antwort auf die NOP-Out-Anforderung gesendet. Wenn der Grenzwert für die No-Op-Zeitüberschreitung erreicht wurde, beendet der Initiator die aktuelle und startet eine neue Sitzung.	Software-iSCSI Abhängige Hardware-iSCSI
ARP-Weiterleitung	Ermöglicht Speichersystemen das dynamische Verschieben von iSCSI-Datenverkehr von einem Port auf einen anderen. ARP wird von Speichersystemen benötigt, die Array-basiertes Failover durchführen.	Software- und unabhängige Hardware-iSCSI (Über die vSphere-CLI konfigurierbar)
Verzögerte Quittierung (ACK)	Ermöglicht Systemen die Verzögerung der Bestätigung empfangener Datenpakete.	Software-iSCSI Abhängige Hardware-iSCSI

Konfigurieren erweiterter Parameter für iSCSI

Die erweiterten iSCSI-Einstellungen steuern Parameter wie „Header-Digest“, „Data Digest“, „ARP-Umleitung“, „Verzögerte Quittierung (ACK)“ usw. In der Regel müssen Sie keine Änderungen an diesen Einstellungen vornehmen, da Ihr ESX/ESXi-Host mit den zugewiesenen vordefinierten Werten funktioniert.

Vorsicht Sie sollten die erweiterten iSCSI-Einstellungen nur ändern, wenn Sie eng mit dem Support-Team von VMware zusammenarbeiten oder anderweitig über umfassende Informationen zu den Werten der einzelnen Einstellungen verfügen.

Vorgehensweise

1 Greifen Sie auf das Dialogfeld „Eigenschaften des iSCSI-Initiators“ zu.

2 Klicken Sie zum Konfigurieren von erweiterten Parametern auf der Initiatorebene auf der Registerkarte „Allgemein“ auf **[Erweitert]** . Fahren Sie mit Schritt 4 fort.

3 Konfigurieren Sie erweiterte Parameter auf der Zielebene.

Auf der Zielebene können erweiterte Parameter nur für Software- und abhängige Hardware-iSCSI-Adapter konfiguriert werden.

a Wählen Sie die Registerkarte **[Dynamische Erkennung]** oder **[Statische Erkennung]** aus.

b Wählen Sie in der Liste der verfügbaren Ziele ein Ziel aus, das Sie konfigurieren möchten, und klicken Sie auf **[Einstellungen] > [Erweitert]** .

4 Geben Sie die erforderlichen Werte für die erweiterten Parameter ein, die Sie ändern möchten, und klicken Sie zum Speichern Ihrer Änderungen auf **[OK]** .

iSCSI-Sitzungsverwaltung

Um miteinander zu kommunizieren, richten iSCSI-Initiatoren und -Ziele iSCSI-Sitzungen ein. Sie können iSCSI-Sitzungen mithilfe der vSphere-CLI prüfen und verwalten.

Standardmäßig starten Software-iSCSI- und abhängige Hardware-iSCSI-Initiatoren eine iSCSI-Sitzung zwischen jedem Initiatorport und jedem Zielport. Wenn Ihr iSCSI-Initiator oder -Ziel über mehrere Ports verfügt, können auf Ihrem Host mehrere Sitzungen eingerichtet sein. Die Standardanzahl an Sitzungen für jedes Ziel entspricht dem Produkt aus der Anzahl an Ports auf dem iSCSI-Adapter und der Anzahl an Zielports. Sie können alle aktuellen Sitzungen anzeigen, um sie zu analysieren und zu debuggen.

Wenn Sie weitere Pfade zu Speichersystemen erstellen möchten, können Sie die Standardanzahl an Sitzungen erhöhen, indem Sie die bestehenden Sitzungen zwischen dem iSCSI-Adapter und den Zielports duplizieren.

Sie können auch eine Sitzung mit einem bestimmten Zielport einrichten. Diese Sitzung kann nützlich sein, wenn Ihr Host eine Verbindung zu einem Speichersystem mit einem einzigen Port herstellt, das Ihrem Initiator standardmäßig nur einen Zielport präsentiert, aber zusätzliche Sitzungen auf einen anderen Zielport umleiten kann. Durch das Einrichten einer neuen Sitzung zwischen Ihrem iSCSI-Initiator und einem anderen Zielport wird ein zusätzlicher Pfad zum Speichersystem erstellt.

Vorsicht Einige Speichersysteme bieten keine Unterstützung für mehrere Sitzungen von demselben Initiatornamen oder Endpunkt aus. Wenn Sie versuchen, mehrere Sitzungen mit solchen Zielen zu erstellen, kann dies zu unvorhersehbarem Verhalten Ihrer iSCSI-Umgebung führen.

Überprüfen von iSCSI-Sitzungen

Verwenden Sie die vSphere-CLI, um iSCSI-Sitzungen zwischen einem iSCSI-Adapter und einem Speichersystem anzuzeigen.

Vorgehensweise

1 Um Sitzungen für einen Adapter aufzulisten, verwenden Sie **`esxcli swiscsi session list –d vmhbaXX`**.

vmhbaXX ist der Name Ihres iSCSI-Adapters.

2 Um Sitzungen für ein Ziel aufzulisten, verwenden Sie **`esxcli swiscsi session list –t iqnXX –d vmhbaXX`**.

iqnXX ist der Name des Ziels, zu dem der iSCSI-Adapter eine Verbindung herstellt.

Beispiel 2-3. Überprüfen von Sitzungen für ein angegebenes Ziel

```
# esxcli swiscsi session list –t iqn.2001–05.com.equallogic:0–8a0906–cbcde0d02–6a445baadf44ab92–vcli7 –d vmhba36
```

Hinzufügen einer iSCSI-Sitzung für ein angegebenes Ziel

Verwenden Sie die vSphere-CLI, um eine iSCSI-Sitzung für ein von Ihnen angegebenes Ziel hinzuzufügen.

Vorgehensweise

1 Verwenden Sie zum Hinzufügen einer Sitzung auf der iSCSI-Adapterebene
`esxcli swiscsi session add –d vmhbaXX`.

vmhbaXX ist der Name Ihres iSCSI-Adapters.

2 Verwenden Sie zum Hinzufügen einer Sitzung auf der Zielebene
`esxcli swiscsi session add –t iqnXX –d vmhbaXX`.

iqnXX ist der Name des Ziels, zu dem der iSCSI-Adapter eine Verbindung herstellt.

Beispiel 2-4. Hinzufügen einer iSCSI-Sitzung für ein angegebenes Ziel

```
# esxcli swiscsi session add –t iqn.2001–05.com.equallogic:0–8a0906–42f9b0401–7d40d28af2a4ade1–
vcli7 –d vmhba36
```

Weiter

Führen Sie eine erneute Prüfung des iSCSI-Adapters durch.

Duplizieren von iSCSI-Sitzungen

Verwenden Sie die vSphere-CLI, um eine iSCSI-Sitzung zwischen einem iSCSI-Adapter und einem Ziel zu duplizieren. Durch das Duplizieren von Sitzungen erhöhen Sie die Standardanzahl an Sitzungen und erstellen zusätzliche Pfade zu Speichersystemen.

Vorgehensweise

- Verwenden Sie zum Duplizieren einer Sitzung
`esxcli swiscsi session add –d vmhbaXX –t iqnXX –s session_isid`.
  - d -- der Name Ihres iSCSI-Adapters, z. B. *vmhbaXX*.
  - t -- Der Name des anzumeldenden Ziels, z. B. *iqnXX*.
  - s -- Die ISID einer zu duplizierenden Sitzung, z. B. *session_isid*. Sie finden diese, indem Sie alle Sitzungen auflisten.

Beispiel 2-5. Duplizieren einer iSCSI-Sitzung

```
# esxcli swiscsi session add –t iqn.2001–05.com.equallogic:0–8a0906–cbcde0d02–6a445baadf44ab92–
vcli7 –s '00:02:3d:00:00:01' –d vmhba36
```

Weiter

Führen Sie eine erneute Prüfung des iSCSI-Adapters durch.

Entfernen von iSCSI-Sitzungen

Verwenden Sie die vSphere-CLI, um eine iSCSI-Sitzung zwischen einem iSCSI-Adapter und einem Ziel zu entfernen.

Vorgehensweise

- Verwenden Sie zum Entfernen einer Sitzung **`esxcli swiscsi session remove`**. Der Befehl verfügt über diese Optionen.
  - d -- der Name Ihres iSCSI-Adapters, z. B. *vmhbaXX*.
  - t -- Der Name des anzumeldenden Ziels, z. B. *iqnXX*.
  - s -- Die ISID einer zu duplizierenden Sitzung, z. B. *session_isid*. Sie finden diese, indem Sie alle Sitzungen auflisten.

Beispiel 2-6. Entfernen einer iSCSI-Sitzung

```
# esxcli swiscsi session remove –t iqn.2001–05.com.equallogic:0–8a0906–cbcde0d02–6a445baadf44ab92–
vcli7 –s '00:02:3d:01:00:01'
```

Weiter

Führen Sie eine erneute Prüfung des iSCSI-Adapters durch.

Hinzufügen von iSCSI-Speicher

Beim Erstellen eines Datenspeichers auf einem iSCSI-Speichergerät führt Sie der Assistent zum Hinzufügen von Speicher durch die Konfiguration.

Vorgehensweise

1. Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenbereich auf den Server.
2. Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend auf **[Speicher]** .
3. Klicken Sie auf **[Speicher hinzufügen]** .
4. Markieren Sie den Speichertyp **[Festplatte/LUN (Disk/LUN)]** , und klicken Sie auf **[Weiter]** .

   Das Dialogfeld **[Festplatte/LUN auswählen (Select Disk/LUN)]** wird angezeigt. Je nach Anzahl der Ziele kann dieser Vorgang einige Sekunden dauern.
5. Wählen Sie das iSCSI-Gerät aus, das Sie für den Datenspeicher verwenden möchten, und klicken Sie auf **[Weiter]** .
6. Überprüfen Sie das aktuelle Layout der Festplatte und klicken Sie auf **[Weiter]** .
7. Geben Sie einen Namen des Datenspeichers ein, und klicken Sie auf **[Weiter]** .

   Der Name des Datenspeichers wird im vSphere-Client angezeigt. Die Bezeichnung muss in der vorliegenden VMware vSphere-Instanz eindeutig sein.
8. Ändern Sie bei Bedarf die Werte für das Dateisystem und die Größe des Datenspeichers.

   Standardmäßig wird der gesamte freie Speicherplatz des Speichergeräts angeboten.
9. Klicken Sie auf **[Weiter]** .

   Die Seite **[Bereit zum Abschließen (Ready to Complete)]** wird angezeigt.
10. Überprüfen Sie die Konfigurationsinformationen für den Datenspeicher, und klicken Sie auf **[Beenden (Finish)]** .

Auf dem iSCSI-Speichergerät ist jetzt ein Datenspeicher verfügbar.

Ändern von SAN-Speichersystemen für ESX/ESXi 3

Nach dem Konfigurieren Ihrer iSCSI-Initiatoren und des Speichers ist es unter Umständen erforderlich, Änderungen an Ihrem Speichersystem vorzunehmen, um eine einwandfreie Funktionsweise mit Ihrer ESX/ESXi-Implementierung zu gewährleisten.

In diesem Abschnitt werden viele der in Verbindung mit VMware ESX/ESXi unterstützten iSCSI-Speichersysteme vorgestellt. Für jedes Gerät werden die wichtigsten bekannten Probleme, Herstellerinformationen (sofern verfügbar) sowie Informationen aus Artikeln der VMware-Knowledgebase aufgeführt.

Hinweis Die in diesem Dokument enthaltenen Informationen werden nur für jede neue Version aktualisiert. Unter Umständen sind neuere Informationen bereits verfügbar. Weitere iSCSI-Speichersysteme werden zwar unterstützt, diese werden jedoch nicht in diesem Kapitel behandelt. Informationen hierzu können Sie dem aktuellen *Handbuch zur SAN-/Speicherkompatibilität* oder den Artikeln der VMware-Knowledgebase entnehmen, oder Sie wenden sich an den Speicheranbieter.

Dieses Kapitel behandelt die folgenden Themen:

- „Testen der ESX/ESXi-SAN-Konfigurationen“, auf Seite 59
- „Allgemeine Überlegungen zu iSCSI-SAN-Speichersystemen“, auf Seite 60
- „EMC CLARiiON-Speichersysteme“, auf Seite 60
- „EMC Symmetrix-Speichersysteme“, auf Seite 61
- „Aktivieren von HP StorageWorks MSA1510i für die Kommunikation mit ESX/ESXi“, auf Seite 62
- „HP StorageWorks EVA-Speichersysteme“, auf Seite 63
- „NetApp-Speichersysteme“, auf Seite 63
- „EqualLogic-Speichersysteme“, auf Seite 66
- „LeftHand Networks SAN/iQ-Speichersysteme“, auf Seite 66
- „Dell PowerVault MD3000i-Speichersysteme“, auf Seite 67
- „iSCSI-Ziele in vApps“, auf Seite 67

Testen der ESX/ESXi-SAN-Konfigurationen

ESX/ESXi Server unterstützt zahlreiche SAN-Speichersysteme mit unterschiedlichen Konfigurationen. VMware testet ESX/ESXi normalerweise mit unterstützten Speichersystemen im Bezug auf die grundlegende Konnektivität, HBA-Failover usw.

Dabei sind nicht alle Speichergeräte für alle Funktionen und Möglichkeiten von ESX/ESXi zertifiziert, und die unterschiedlichen Anbieter haben ggf. spezifische Schwerpunkte im Hinblick auf den Support für ESX/ESXi.

VMware testet ESX/ESXi mit folgenden Speichersystemkonfigurationen:

Grundlegende Konnektivität	Es wird getestet, ob ESX/ESXi das Speichersystem erkennt und damit ausgeführt werden kann. Bei dieser Konfiguration sind Multipathing oder andere Failover-Arten nicht zulässig.
iSCSI-Failover	Der Server ist mit mehreren iSCSI-HBAs oder -Netzwerkkarten ausgestattet. Der Server arbeitet bei HBA- oder Netzwerkkartenausfällen zuverlässig weiter.
Speicherport-Failover	Der Server ist mehreren Speicherports angehängt und verhält sich bei Speicherport- und Switch-Ausfällen zuverlässig.
Starten über ein SAN (nur mit ESX-Hosts)	Der ESX-Host startet von einer über einen SAN konfigurierten LUN und nicht vom Server aus.

Allgemeine Überlegungen zu iSCSI-SAN-Speichersystemen

Wenn Sie Ihr iSCSI-SAN-Speichersystem für den Einsatz mit ESX/ESXi vorbereiten, müssen Sie spezifische Anforderungen beachten, die für alle Speichersysteme gelten.

Die folgenden allgemeinen Anforderungen gelten für alle Speichersysteme:

- LUNs müssen für jeden HBA auf jedem Host mit der gleichen LUN-ID-Nummer bereitgestellt werden. Bei Verwendung unterschiedlicher Nummern erkennt der ESX/ESXi-Host keine unterschiedlichen Pfade zu derselben LUN. Da die Anweisungen zur Konfiguration identischer SAN-LUN-IDs Hersteller-abhängig sind, sollten Sie weitere Informationen zu diesem Thema der Dokumentation Ihres Speichers entnehmen.
- Legen Sie, sofern für bestimmte Speichersysteme in diesem Kapitel keine abweichenden Angaben gemacht werden, für den Hosttyp für LUNs, die für den ESX/ESXi verfügbar sind, `Linux oder Linux–Cluster` fest, sofern in Ihrem Speichersystem verfügbar. Das vom ESX/ESXi angewandte Verfahren zum Zugreifen auf das Speichersystem ist meist mit dem Linux-Zugriff kompatibel, wobei hier das von Ihnen verwendete Speichersystem ausschlaggebend ist.
- Wenn Sie VMotion, DRS oder HA verwenden, stellen Sie sicher, dass für Quell- und Zielhosts für virtuelle Maschinen die gleichen LUNs mit identischen LUN-IDs verfügbar sind. SAN-Administratoren mag es unüblich erscheinen, mehreren Hosts die gleichen LUNs bereitzustellen, da sie besorgt sind, dass dies zu einer Datenbeschädigung führen könnte. VMFS verhindert jedoch den gleichzeitigen Schreibvorgang mehrerer virtueller Maschinen in die gleiche Datei, und daher können die LUNs allen erforderlichen ESX/ESXi-Systemen bereitgestellt werden.
- Wenn für die LUNs, auf die zugegriffen wird, keine CHAP-Authentifizierung festgelegt wurde, müssen Sie CHAP auf dem ESX/ESXi-Host ebenfalls deaktivieren. Anderenfalls schlägt die Authentifizierung des Speichersystems fehl, obwohl für die LUNs keine CHAP-Anforderungen bestehen.

EMC CLARiiON-Speichersysteme

EMC CLARiiON-Speichersysteme arbeiten mit ESX/ESXi-Hosts in iSCSI SAN-Konfigurationen. Verwenden Sie in der Regel die EMC-Software zum Durchführen der Konfiguration.

Weitere Informationen finden Sie in der EMC-Dokumentation.

Hierbei handelt es sich um ein Aktiv/Passiv-Festplatten-Array, sodass alle Probleme im Zusammenhang mit Aktiv/Passiv-Festplatten-Arrays relevant sind. Beachten Sie weiterhin Folgendes:

- Um ein Pfad-Thrashing zu verhindern, ist die Multipathing-Richtlinie standardmäßig auf **[Zuletzt verwendet (Most Recently Used)]** und nicht auf **[Fest (Fixed)]** gesetzt. Das ESX/ESXi-System legt die Standardrichtlinie fest, sobald ein Speichersystem ermittelt wird.
- Um einen Startvorgang von einem SAN durchzuführen, wählen Sie den aktiven Speicherprozessor für das Ziel der Start-LUN im HBA-BIOS.
- Auf EMC CLARiiON AX100i- und AX150i-Systemen werden RDMs nur unterstützt, wenn Sie die Navisphere Management Suite für die SAN-Verwaltung verwenden. Es wird jedoch keine Garantie übernommen, dass Navisphere Express diese ordnungsgemäß konfiguriert.

  Eine erfolgreiche Verwendung von RDMs setzt voraus, dass für eine bestimmte LUN für jeden ESX/ESXi-Host im Cluster die gleiche LUN-ID verwendet wird. Bei den Systemen AX100i und AX150i wird standardmäßig nicht auf diese Weise verfahren.
- Wenn Sie ein AX100i- oder AX150i-Speichersystem verwenden, nimmt kein Host-Agent in regelmäßigen Abständen eine Überprüfung der Hostkonfiguration vor, und Änderungen werden nicht an das Speichersystem weitergeleitet. Das Dienstprogramm `axnaviserverutil cli` wird zum Update der Änderungen verwendet. Hierbei handelt es sich um einen manuellen Vorgang, der bei Bedarf durchgeführt wird.
- Zum Unterstützen von Port-Binding auf EMC CLARiiON-Speichersystemen sind Initiatoren in verschiedenen Subnetzen erforderlich. Weitere Informationen hierzu finden Sie in der Dokumentation des Anbieters.
- Um sicherzugehen, dass ESX/ESXi EMC CLARiiON mit ALUA unterstützt, überprüfen Sie die HCLs, um sicherzustellen, dass die richtige Firmware-Version für das Speicher-Array verwendet wird. Weitere Informationen erhalten Sie von Ihrem Speicheranbieter.

EMC Symmetrix-Speichersysteme

EMC Symmetrix-Speichersysteme benötigen bestimmte Einstellungen, um mit ESX/ESXi arbeiten zu können. Verwenden Sie EMC-Software, um das Speichersystem zu konfigurieren. Weitere Informationen finden Sie in der EMC-Dokumentation.

Für ESX/ESXi-Vorgänge auf einem Symmetrix-Netzwerkspeichersystem sind folgende Einstellungen erforderlich:

- Allgemeine Seriennummer (C)
- Automatische Aushandlung (EAN) aktiviert
- SCSI 3 (SC3) festgelegt (aktiviert)
- Eindeutiger World Wide Name (UWN)
- SPC-2 (Decal) (SPC2) SPC-2-Flag ist erforderlich

HINWEIS ESX/ESXi-Host betrachten LUNs eines Symmetrix-Speichersystems, die über eine Kapazität von 50 MB oder weniger verfügen, als Verwaltungs-LUNs. Diese LUNs werden auch als Pseudo-LUNs oder Gatekeeper-LUNs bezeichnet. Sie werden auf der EMC Symmetrix-Verwaltungsschnittstelle dargestellt, sollten jedoch nicht zum Speichern von Daten verwendet werden.

Aktivieren von HP StorageWorks MSA1510i für die Kommunikation mit ESX/ESXi

In diesem Abschnitt werden die Schritte für das Setup und die Konfiguration beschrieben, die erforderlich sind, um die Kommunikation des HP StorageWorks MSA1510i-Speichersystems mit ESX Hosts zu ermöglichen.

Vorgehensweise

1 Installieren und verbinden Sie die Netzwerkgeräte entsprechend den Installationsanweisungen des Anbieters, und schalten Sie sie ein.

2 Ermitteln Sie die IP-Adresse, die dem Verwaltungsport des MSA1510i-Controllers zugeordnet ist.

   a Gehen Sie die Meldungen auf dem LCD-Bildschirm durch, bis folgende Meldung angezeigt wird: `603 Port MA0 IP` *`Adresse`*

   b Notieren Sie die unter den **[grundlegenden MSA1510i-Informationen]** aufgeführte IP-Adresse des Verwaltungsports.

3 Öffnen Sie vom Server oder einer Workstation aus im MSA1510i LAN-Segment einen Webbrowser, und geben Sie die in Schritt 2 besorgte Adresse ein.

4 Geben Sie bei Aufforderung die Standardzugriffsberechtigungen ein.

   - Benutzername: `Root`
   - Kennwort: `Root`

5 Legen Sie bei Aufforderung einen eindeutigen Benutzernamen und ein eindeutiges Kennwort fest.

6 Schließen Sie mithilfe des Assistenten die folgenden Vorgänge ab.

Option	Beschreibung
Speicherkonfiguration	a Legen Sie den Fehlertoleranzmodus (RAID-Modus) fest. b Weisen Sie der entsprechenden RAID-Ebene ungenutzten Speicherplatz zu.
iSCSI-Konfiguration (Konfigurieren eines iSCSI-Portals)	a Wählen Sie einen Datenport. b Weisen Sie dem Datenport eine IP-Adresse zu. c VLANs werden auf dem Switch eingerichtet und als eine Methode zur Steuerung des Speicherzugriffs verwendet. Wenn Sie VLANs verwenden, geben Sie die zu verwendende VLAN-ID ein (0 = nicht verwendet). d Der Assistent schlägt einen standardmäßigen iSCSI-Zielnamen und einen iSCSI-Zielalias vor. Übernehmen Sie die Standardwerte, oder geben Sie benutzerdefinierte Werte ein. **Hinweis** Um die verbleibenden Datenports zu konfigurieren, schließen Sie den Assistenten für die erste Systemkonfiguration ab, und verwenden Sie die auf der Registerkarte **[Konfigurieren (Configure)]** verfügbaren Aufgaben.
Anmeldeeinstellungen	Geben Sie die Anmeldeeinstellungen ein.
Verwaltungseinstellungen	Geben Sie die Verwaltungseinstellungen ein.

7 Klicken Sie auf **[Beenden (Finish)]**, um die Konfigurationseinstellungen zu übernehmen.

Hinweis Assistenten stehen nur für grundlegende Konfigurationsaufgaben zur Verfügung. Verwenden Sie die Registerkarten **[Verwalten]** und **[Konfigurieren]**, um die Konfiguration zu überprüfen und Änderungen daran vorzunehmen.

Weiter

Führen Sie nach der ersten Einrichtung die folgenden Aufgaben zum Abschließen der Konfiguration durch:

- Erstellen Sie ein Array.
- Erstellen Sie ein logisches Laufwerk.
- Erstellen Sie ein Ziel.
- Erstellen Sie eine Portalgruppe.
- Verbinden Sie die erstellten Portale mithilfe des Assistenten mit der erstellten Portalgruppe, oder weisen Sie diese zu.
- Ordnen Sie dem Ziel logische Laufwerke zu.
- Fügen Sie Initiatoren hinzu (IQN-Name und Alias des Initiators).
- Aktualisieren Sie die ACLs der logischen Laufwerke, um Zugriff auf die Initiatoren bereitzustellen (wählen Sie die Liste der Initiatoren, um auf das logische Laufwerk zuzugreifen).

HP StorageWorks EVA-Speichersysteme

Bei den beiden Arten des HP StorageWorks-EVA-Systems handelt es sich um EVA_GL, ein Aktiv/Passiv-System, und EVA_XL, ein Aktiv/Aktiv-System. Der Einsatz von ESX/ESXi auf Systemen setzt die folgenden Einstellungen voraus.

Legen Sie für den Verbindungstyp **[Benutzerdefiniert (Custom)]** fest, wenn Sie eine LUN für einen ESX/ESXi-Host bereitstellen. Hierbei wird einer der folgenden Werte verwendet:

- Verwenden Sie für HP EVAgl 3000/5000 (Aktiv/Passiv) den Hostmodustyp `000000002200282E`.
- Verwenden Sie für HP EVAgl Firmware 4.001 (Aktiv/Aktiv-Firmware für die GL-Serie) und höher den Hostmodustyp `VMware`.
- Verwenden Sie für EVA4000/6000/8000-Aktiv/Aktiv-Arrays mit Firmwareversionen vor 5.031 den Hostmodustyp `000000202200083E`.
- Verwenden Sie für EVA4000/6000/8000-Aktiv/Aktiv-Arrays mit Firmware der Version 5.031 und höher den Hostmodustyp `VMware`.

Anderenfalls sind für EVA-Systeme zum Ausführen mit einem ESX/ESXi-System keine besonderen Konfigurationsänderungen erforderlich.

NetApp-Speichersysteme

Zur Kommunikation zwischen NetApp-Speichersystemen in einer ESX/ESXi -Umgebung sind bestimmte Konfigurationsschritte erforderlich.

Zusätzliche Dokumentation zu NetApp- und VMware-Best-Practices sowie zu SAN-Lösungen finden Sie auf der Webseite von NetApp.

Tabelle 3-1. Konfigurationsschritte

Konfigurationsschritt	Beschreibung
Deaktivieren Sie ALUA.	Wenn einer Ihrer iSCSI-Initiatoren Teil der Initiatorgruppe sind (igroup), deaktivieren Sie ALUA auf dem NetApp-Filter.
Richten Sie Multipathing ein.	Wenn Sie Multipathing zwischen zwei iSCSI-HBAs und mehreren Ports in einem NetApp-Speichersystem einrichten, weisen Sie den beiden HBAs unterschiedliche dynamische oder statische Erkennungsadressen zu, um eine Verbindung mit dem Speicher herzustellen. Das NetApp-Speichersystem erlaubt nur eine Verbindung für jedes Ziel und jeden Initiator. Wenn Sie versuchen, weitere Verbindungen aufzubauen, bricht die erste Verbindung ab. Daher sollte ein einzelner HBA nicht versuchen, eine Verbindung mit mehreren IP-Adressen herzustellen, die mit dem gleichen Network Appliance-Ziel verbunden sind.
Legen Sie den LUN-Typ und den Initiatorgruppentyp fest.	Legen Sie für das Speichersystem den geeigneten LUN- und Initiatorgruppentyp fest: ■ LUN-Typ (LUN Type) – VMware (verwenden Sie Linux, wenn der Typ VMware nicht verfügbar ist). ■ Initiatorgruppentyp (Initiator Group Type) – VMware (verwenden Sie Linux, wenn der Typ VMware nicht verfügbar ist).
Stellen Sie den Speicher bereit.	Verwenden Sie entweder FilerView oder CLI.

Bereitstellen von Speicher mithilfe der FilerView-Speicherverwaltung

Sie können FilerView verwenden, um Speicher auf einem NetApp-Speichersystem bereitzustellen.

Vorgehensweise

1 Melden Sie sich bei der NetApp-Speichersystemverwaltung (FilerView) an.

2 Erstellen Sie ein Volume.

   a Wählen Sie **[Volumes]** , und klicken Sie auf **[Hinzufügen (Add)]** .

   b Klicken Sie auf **[Weiter]** .

   c Wählen Sie **[Flexibilität (Flexibility)]** (Standard) oder **[Herkömmlich (Traditional)]** , und klicken Sie anschließend auf **[Weiter]** .

   d Geben Sie einen **[Volume-Namen (Volume Name)]** ein, wählen Sie eine **[Sprache (Language)]** , und klicken Sie auf **[Weiter]** .

   e Geben Sie Werte für **[Enthält Zusammenstellung (Containing Aggregate)]** , **[Gesamt-Volume-Größe (Total Volume Size)]** und **[Garantierter Speicher (Space Guarantee)]** ein, und klicken Sie auf **[Weiter]** .

   f Klicken Sie auf **[Übernehmen (Commit)]** , um das Volume zu erstellen.

3 Erstellen Sie LUNs.

   a Wählen Sie **[LUNs]** , und klicken Sie auf **[Hinzufügen (Add)]** .

   b Geben Sie Folgendes ein:

   - **[Pfad (Path)]** : Geben Sie einen Pfad ein, wie z.B. `/vol/vol1/lun1`.
   - **[LUN-Protokolltyp (LUN Protocol Type)]** : VMware.
   - **[Beschreibung (Description)]** : Eine kurze Beschreibung.
   - **[Größe und Einheit (Size and Unit)]** : Geben Sie eine Größe wie beispielsweise 10 GB ein, und wählen Sie **[Reservierter Platz (Space Reserved)]** .

4 Erstellen Sie eine Initiatorgruppe.

   a Wählen Sie **[LUNs] > [Initiatorgruppe (Initiator Group)]** , und klicken Sie anschließend auf **[Hinzufügen (Add)]** .

   b Geben Sie Folgendes ein:

   - **[Gruppenname (Group Name)]** : Geben Sie einen Gruppennamen ein.
   - **[Typ (Type)]** : Wählen Sie **[iSCSI]** .
   - **[Betriebssystem (Operating System)]** : Geben Sie **`VMware`** ein.
   - **[Initiatoren (Initiators)]** : Geben Sie vollständig qualifizierte Initiatornamen ein. Wenn mehrere Initiatoren vorhanden sind, müssen die einzelnen Initiatoren durch Betätigen der Eingabetaste voneinander getrennt werden.

   c Klicken Sie auf **[Hinzufügen]** .

5 Ordnen Sie die LUN der Initiatorgruppe zu.

   a Wählen Sie **[LUNs]** , und klicken Sie auf **[Verwalten (Manage)]** .

   Eine Liste mit LUNs wird angezeigt.

   b Klicken Sie in dieser Liste in der Zeile **[Zuordnungen (Maps)]** auf die Bezeichnungen für die verschiedenen LUNs.

   c Klicken Sie auf **[Gruppen zu Zuordnung hinzufügen (Add Groups to Map)]** .

   d Wählen Sie die Initiatorgruppe, und klicken Sie auf **[Hinzufügen (Add)]** .

   e Geben Sie bei Aufforderung die LUN-ID (eine beliebige Zahl zwischen 0 und 255) ein, und klicken Sie auf **[Übernehmen]** .

Bereitstellen von Speicher über die Befehlszeilenschnittstelle

Sie können die Befehlszeilenschnittstelle verwenden, um auf einem NetApp-Speichersystem Speicher bereitzustellen.

Vorgehensweise

1 Erstellen Sie bei Bedarf mithilfe der Befehlszeilenschnittstelle eine Zusammenstellung.

```
aggr create vmware–aggrnumber of disks
```

2 Erstellen Sie ein flexibles Volume.

```
vol create aggregate namevolume size
```

3 Erstellen Sie ein Qtree zum Speichern jeder LUN.

```
qtree create path
```

4 Erstellen Sie eine LUN.

```
lun create –s size –t vmware path
```

5 Erstellen Sie eine Initiatorgruppe.

```
igroup create –f –t vmware igroup name
```

6 Ordnen Sie die LUN der von Ihnen erstellen Initiatorgruppe zu.

```
lun map (path) igroup nameLUN ID
```

EqualLogic-Speichersysteme

Um Ihr EqualLogic-Speichersystem für die Ausführung mit einer ESX/ESXi-Implementierung einzurichten, ist Folgendes zu beachten:

Im Folgenden finden Sie eine Auflistung mit Anforderungen an das EqualLogic-Speichersystem, die beim Ensatz von ESX/ESXi erforderlich sind:

- Multipathing. Hierfür ist keine besondere Einrichtung erforderlich, da EqualLogic-Speichersysteme Failover von Speicherprozessoren unterstützen, die für iSCSI transparent sind. Mehrere iSCSI-HBAs oder -Netzwerkkarten können eine Verbindung mit dem gleichen Ziel oder der gleichen LUN auf Speicherseite herstellen.
- Erstellen von iSCSI-LUNs. Klicken Sie im Internetportal von EqualLogic mit der rechten Maustaste auf **[Volumes]** , und wählen Sie dann **[Volume erstellen (Create Volume)]** .
- Aktivieren Sie die ARP-Umleitunge für ESX/ESXi-Hardware-iSCSI-HBAs.
- EqualLogic-Speichersysteme geben eine Obergrenze von 512 iSCSI-Verbindungen pro Speicherpool und 2048-Verbindungen pro Speichergruppe vor.

Weitere Informationen zum Konfigurieren und Verwenden von EqualLogic-Speichersystemen finden Sie in der Dokumentation des Anbieters.

LeftHand Networks SAN/iQ-Speichersysteme

SAN/iQ-SANs unterstützen ESX/ESXi-iSCSI-Verbindungen von einem Software- und einem Hardware-Initiator.

Aktivieren Sie bei der Konfiguration von SAN/iQ eine automatische Volume-Neusignierung für SAN/iQ-Speichergeräte, um Zugriff auf SAN/iQ-Snapshots und Remotekopien zu ermöglichen.

Weitere Informationen zum Konfigurieren von LeftHand Networks-SANs für VMware vSphere finden Sie in der VMware-Herstellerdokumentation.

Grundelegende Schritte beinhalten verschiedene Aufgaben.

1 Installieren von SAN/iQ-Speicherknoten

2 Erstellen von SAN/iQ-Verwaltungsgruppen und Clustern

3 Erstellen von Volumes

4 Zuweisen von Volumes zu Authentifizierungsgruppen und Volume-Listen

5 Aktivieren der ARP-Umleitung für Hardware-iSCSI-HBAs.

Es wird empfohlen, einen virtuellen IP-Lastausgleich in SAN/iQ für alle ESX/ESXi-Authentifizierungsgruppen zu konfigurieren.

Dell PowerVault MD3000i-Speichersysteme

Bei der Konfiguration von beidseitigem CHAP für die MD3000i iSCSI-Speichergeräte sollten Sie bestimmte Überlegungen anstellen.

Beachten Sie beim Konfigurieren von beidseitigem CHAP für das MD3000i iSCSI-Array die folgenden Richtlinien:

- Auf dem MD3000i-Speichersystem benötigt die beidseitige CHAP-Konfiguration lediglich einen CHAP-Schlüssel.
- Auf dem ESX/ESXi-Host ist für die beidseitige CHAP-Konfiguration der Name und der CHAP-Schlüssel erforderlich. Geben Sie bei der Konfiguration von beidseitigem CHAP auf dem ESX/ESXi-Host den IQN-Namen des Ziels als den Namen für das beidseitge CHAP ein. Stellen Sie sicher, dass der CHAP-Schlüssel mit demjenigen auf dem Array übereinstimmt.

iSCSI-Ziele in vApps

Wenn Sie ein iSCSI-Ziel in einer virtuellen Appliance verwenden, z. B. HP LeftHand P4000 VSA, sollte der Host über den Software-iSCSI-Adapter und nicht über einen Hardware-iSCSI-Adapter mit dem Ziel verbunden werden.

Starten von einem iSCSI-SAN

4

Wenn Sie Ihren Host so einrichten, dass er von einem SAN gestartet wird, wird das Start-Image des Hosts auf einer oder mehreren LUNs im SAN-Speichersystem gespeichert. Wenn der Host startet, wird er nicht von seiner lokalen Festplatte aus, sondern von der LUN im SAN aus gestartet.

Sie können das Starten vom SAN verwenden, wenn Sie keinen lokalen Speicher warten möchten oder Hardwarekonfigurationen ohne Festplatten haben, wie z. B. Blade-Systeme.

ESX- und ESXi-Hosts unterstützen verschiedene Methoden zum Starten vom SAN.

Tabelle 4-1. Unterstützung für das Starten vom iSCSI-SAN

Hosttyp	Unabhängige Hardware-iSCSI	Software-iSCSI und abhängige Hardware-iSCSI
ESX-Host	Wird unterstützt. Für das Starten vom SAN ist ein iSCSI-HBA erforderlich.	Nicht unterstützt.
ESXi-Host	Nicht unterstützt.	Wird unterstützt. Der Netzwerkadapter muss die iBFT unterstützen.

Das Starten Ihres Hosts von einem SAN bietet zahlreiche Vorteile.

- Günstigere Server. Höhere Serverdichte und bessere Ausführung ohne internen Speicher.
- Einfacherer Serveraustausch. Sie können Server problemlos austauschen und den neuen Server so einrichten, dass sie auf den alten Speicherort der Start-Image-Datei verweisen.
- Weniger ungenutzter Speicherplatz.
- Einfachere Sicherungsvorgänge. Die Systemstart-Images im SAN können als Teil der allgemeinen SAN-Sicherungsverfahren gesichert werden.
- Verbesserte Verwaltung. Das Erstellen und Verwalten des Betriebssystem-Images ist einfacher und effizienter.

Dieses Kapitel behandelt die folgenden Themen:

- „Allgemeine Empfehlungen für das Starten von einem iSCSI-SAN“, auf Seite 70
- „Vorbereiten des iSCSI-SAN“, auf Seite 70
- „Konfigurieren von ESX-Hosts für das Starten über ein iSCSI-SAN“, auf Seite 71
- „iBFT-iSCSI-Start - Überblick“, auf Seite 72
- „Erfassen von Diagnoseinformationen für ESXi-Hosts“, auf Seite 77

Allgemeine Empfehlungen für das Starten von einem iSCSI-SAN

Wenn Sie eine iSCSI-LUN als Startgerät für Ihren Host einrichten und verwenden möchten, müssen Sie einige allgemeine Richtlinien befolgen.

Diese Richtlinien gelten für das Starten von Software und abhängigem iSCSI sowie für unabhängige Hardware-iSCSI.

- Prüfen Sie die Herstellerempfehlungen für die Hardware, die Sie in Ihrer Startkonfiguration verwenden.
- Weitere Informationen zu den Voraussetzungen und Anforderungen finden Sie im entsprechenden ESX/ESXi-Installationshandbuch.
- Verwenden Sie statische IP-Adressen, um das Auftreten von DHCP-Konflikten zu vermeiden.
- Verwenden Sie für VMFS-Datenspeicher und Startpartitionen verschiedene LUNs.
- Konfigurieren Sie auf Ihrem Speichersystem ordnungsgemäße ACLs.
  - Die Start-LUN sollte nur für den Host sichtbar sein, der die LUN verwendet. Auf diese Start-LUN sollten andere Hosts im SAN nicht zugreifen dürfen.
  - Wenn eine LUN für einen VMFS-Datenspeicher verwendet wird, kann sie von mehreren Hosts gemeinsam verwendet werden. Dies wird durch ACLs im Speichersystem ermöglicht.
- Konfigurieren Sie eine Diagnosepartition.
  - Nur bei unabhängigen Hardware-iSCSI können Sie die Diagnosepartition auf der Start-LUN platzieren. Wenn Sie die Diagnosepartition in der Start-LUN konfigurieren, kann diese LUN nicht von mehreren Hosts verwendet werden. Wenn eine separate LUN für eine Diagnosepartition verwendet wird, kann sie von mehreren Hosts gemeinsam verwendet werden.
  - Wenn Sie einen ESXi-Host vom SAN mithilfe von iBFT starten, können Sie keine Diagnosepartition auf einer SAN-LUN einrichten. Verwenden Sie stattdessen den vSphere Management Assistant (vMA), um Diagnoseinformationen von Ihrem Host zu erfassen und für die anschließende Analyse zu speichern.

    Weitere Informationen hierzu finden Sie unter „Erfassen von Diagnoseinformationen für ESXi-Hosts“, auf Seite 77.

Vorbereiten des iSCSI-SAN

Bevor Sie Ihren ESX/ESXi-Host zum Starten von einer iSCSI-LUN konfigurieren, müssen Sie Ihr SAN vorbereiten und konfigurieren.

Vorsicht Wenn Sie über ein SAN starten und die Installation von ESX per Skript erfolgt, müssen Sie bestimmte Schritte ausführen, um einen unerwünschten Datenverlust zu vermeiden.

Vorgehensweise

1 Schließen Sie die Netzwerkkabel an, wie in den Handbüchern der betreffenden Geräte beschrieben.

2 Stellen Sie die IP-Verbindung zwischen dem Speichersystem und dem Server sicher.

Hierzu gehört ebenfalls die ordnungsgemäße Konfiguration aller Router und Switches im Speichernetzwerk. Speichersysteme müssen ein Ping-Signal an die iSCSI-Adapter in den Hosts senden können.

3 Konfigurieren Sie das Speichersystem.

a Erstellen Sie ein Volume (oder eine LUN) im Speichersystem für Ihren Host, von dem gebootet werden soll.

b Konfigurieren Sie das Speichersystem, sodass Ihr Host auf die zugewiesene LUN zugreifen kann.

Hierzu ist möglicherweise ein Update der ACLs mit den IP-Adressen, den iSCSI-Namen und dem CHAP-Authentifizierungsparameter, den Sie auf Ihrem Host verwenden, erforderlich. Auf einigen Speichersystemen müssen Sie zusätzlich zu den Zugriffsdaten für den ESX/ESXi-Host auch ausdrücklich die zugewiesene LUN mit dem Host verknüpfen.

c Stellen Sie sicher, dass die LUN dem Host ordnungsgemäß präsentiert wird.

d Stellen Sie sicher, dass kein anderes System auf die konfigurierte LUN zugreifen kann.

e Schreiben Sie sich den iSCSI-Namen und die IP-Adresse der Ziele auf, die dem Host zugewiesen sind.

Sie benötigen diese Informationen für die Konfiguration Ihrer iSCSI-Adapter.

Konfigurieren von ESX-Hosts für das Starten über ein iSCSI-SAN

Sie können den ESX-Host nur über das iSCSI-SAN starten, wenn der Host einen unabhängigen Hardware-iSCSI-Adapter verwendet, wie z. B. einen QLogic-HBA. Sie müssen den unabhängigen Hardware-iSCSI-Adapter zum Starten über das SAN konfigurieren.

Dieses Verfahren erläutert, wie der QLogic-iSCSI-HBA für das Starten vom SAN aktiviert wird. Weitere Informationen und aktuelle Einzelheiten zu den QLogic-Adapter-Konfigurationseinstellungen finden Sie auf der QLogic-Website.

Voraussetzungen

Da Sie zuerst vom VMware-Installationsmedium starten müssen, richten Sie Ihren Host so ein, dass er von DVD-ROM startet. Ändern Sie hierzu die Startreihenfolge in den BIOS-Einstellungen des Systems.

Vorgehensweise

1 Legen Sie die Installations-DVD in das DVD-ROM-Laufwerk ein und starten Sie den Host neu.

2 Stellen Sie im BIOS ein, dass der Host zuerst vom DVD-ROM-Laufwerk aus gestartet wird.

3 Drücken Sie während des Server-POST die Tastenkombination Strg+q, um das QLogic-iSCSI-HBA-Konfigurationsmenü zu öffnen.

4 Wählen Sie den zu konfigurierenden E/A-Port.

Standardmäßig ist **[Adapterstartmodus (Adapter Boot Mode)]** auf **[Deaktivieren (Disable)]** gesetzt.

5 Konfigurieren Sie den HBA.

a Wählen Sie aus dem Menü **[Fast!UTIL-Optionen (Fast!UTIL Options)]** die Option **[Konfigurationseinstellungen (Configuration Settings)] > [Host Adapter Settings (Hostadaptereinstellungen)]** aus.

b Konfigurieren Sie die folgenden Einstellungen für Ihren Hostadapter: Initiator-IP-Adresse, Subnetzmaske, Gateway, Initiator-iSCSI-Name und CHAP (falls erforderlich).

6 Konfigurieren Sie die iSCSI-Einstellungen.

Weitere Informationen hierzu finden Sie unter „Konfigurieren der iSCSI-Starteinstellungen“, auf Seite 72.

7 Speichern Sie die Änderungen, und starten Sie das System neu.

Konfigurieren der iSCSI-Starteinstellungen

Sie müssen beim Einrichten Ihres ESX-Hosts zum Starten von iSCSI die iSCSI-Starteinstellungen konfigurieren.

Vorgehensweise

1 Wählen Sie aus dem Menü **[Fast!UTIL Options]** die Option **[Configuration Settings] > [iSCSI Boot Settings]** aus.

2 Bevor Sie SendTargets festlegen können, setzen Sie **[Adapter Boot mode]** auf **[Manual]** .

3 Aktivieren Sie **[Primary Boot Device Settings]** .

a Geben Sie **[Target IP]** und **[Target Port]** für die Zielerkennung ein.

b Die Felder **[Boot LUN]** und **[iSCSI Name]** müssen nicht ausgefüllt werden, wenn nur ein iSCSI-Ziel und eine LUN für die angegebene Adresse vorhanden sind, über die der Start erfolgen soll. Anderenfalls müssen Sie diese Felder ausfüllen, um sicherzustellen, dass der Start nicht über ein Volume oder ein anderes System durchgeführt wird. Nachdem das Zielspeichersystem erreicht wurde, werden diese Felder nach einem erneuten Prüfen ausgefüllt angezeigt.

c Speichern Sie die Änderungen.

4 Wählen Sie im Menü **[iSCSI Boot Settings]** das primäre Startgerät. Zur Suche nach neuen Ziel-LUNs wird ein erneuter Prüfvorgang des HBA ausgeführt.

5 Wählen Sie das iSCSI-Ziel.

HINWEIS Wenn mehr als eine LUN im Ziel vorhanden ist, können Sie eine bestimmte LUN-ID wählen, indem Sie nach Auswahl des iSCSI-Gerätes die **[Eingabetaste]** drücken.

6 Öffnen Sie das Menü **[Primary Boot Device Setting]** . Nach der erneuten Prüfung sind die Felder **[Boot LUN]** und **[iSCSI Name]** ausgefüllt. Ändern Sie den Wert von **[Boot LUN]** in die gewünschte LUN-ID.

iBFT-iSCSI-Start - Überblick

ESXi-Hosts können mithilfe von Software- oder abhängigen Hardware-iSCSI-Adaptern und Netzwerkadaptern von einer iSCSI-SAN gestartet werden.

Der Host muss über einen Netzwerkadapter verfügen, der das Starten von iSCSI und das iBFT-Format (iBFT, iSCSI Boot Firmware Table) unterstützt, um ESXi bereitzustellen und vom iSCSI-SAN starten zu können. Die iBFT ist eine Methode zur Übermittlung von Parametern zum iSCSI-Startgerät an ein Betriebssystem.

Bevor Sie ESXi installieren und vom iSCSI-SAN starten, konfigurieren Sie das Netzwerk und die iSCSI-Startparameter auf dem Netzwerkadapter und aktivieren Sie den Adapter für das Starten von iSCSI. Da die Konfiguration des Netzwerkadapters herstellerabhängig ist, lesen Sie die Anweisungen in der Dokumentation Ihres Herstellers.

Beim ersten Starten über iSCSI verbindet sich die iSCSI-Start-Firmware auf Ihrem System mit einem iSCSI-Ziel. Wenn die Anmeldung erfolgreich ist, speichert die Firmware die Netzwerk- und iSCSI-Start-Parameter in der iBFT und die Tabelle im Arbeitsspeicher des Systems. Das System verwendet diese Tabelle zur Konfiguration seiner eigenen iSCSI-Verbindung und seines iSCSI-Netzwerks sowie zum Starten.

Die iBFT-iSCSI-Startsequenz wird in der folgenden Liste beschrieben.

1 Beim Neustart erkennt das System-BIOS die iSCSI-Start-Firmware auf dem Netzwerkadapter.

2 Die iSCSI-Start-Firmware verwendet zum Verbinden mit dem angegebenen iSCSI-Ziel die vorkonfigurierten Startparameter.

3 Wenn die Verbindung mit dem iSCSI-Ziel hergestellt wurde, schreibt die iSCSI-Start-Firmware die Netzwerk- und iSCSI-Startparameter in die iBFT und speichert die Tabelle im Systemarbeitsspeicher.

Hinweis Das System verwendet diese Tabelle zur Konfiguration seiner eigenen iSCSI-Verbindung und seines iSCSI-Netzwerks sowie zum Starten.

4 Das BIOS startet das Startgerät.

5 Der VMkernel startet den Ladevorgang und übernimmt den Startvorgang.

6 Der VMkernal verwendet die Startparameter aus der iBFT zum Herstellen einer Verbindung mit dem iSCSI-Ziel.

7 Nach Herstellung der iSCSI-Verbindung wird das System gestartet.

iBFT-iSCSI-Start - Überlegungen

Es gelten gewisse Erwägungen, wenn Sie mithilfe von iBFT-aktivierten Netzwerkadaptern einen ESXi-Host von iSCSI starten.

Der iBFT-iSCSI-Startvorgang unterstützt Folgendes nicht:

- IPv6
- Failover für die iBFT-aktivierten Netzwerkadapter

Hinweis Aktualisieren Sie mithilfe der vom Anbieter bereitgestellten Tools den Startcode Ihrer Netzwerkkarte und die iBFT-Firmware, bevor Sie versuchen, VMware ESXi 4.1 zu installieren und zu starten. Informationen über den unterstützten Startcode und die iBFT-Firmware-Versionen zum Starten von VMware ESXi 4.1 finden Sie in der Herstellerdokumentation und dem VMware HCL-Handbuch. Der Startcode und die iBFT-Firmware, die von den Herstellern vor ESXi 4.1 freigegeben wurden, funktionieren möglicherweise nicht.

Nach dem Einrichten des Hosts für das Starten von iBFT-iSCSI gelten die folgenden Einschränkungen:

- Sie können den Software-iSCSI-Adapter nicht deaktivieren. Wenn die iBFT-Konfiguration im BIOS vorhanden ist, aktiviert der Host den Software-iSCSI-Adapter bei jedem Neustart neu.
- Sie können das iBFT-iSCSI-Startziel nicht mithilfe des vSphere-Clients entfernen. Das Ziel erscheint auf der Liste der statischen Ziele des Adapters.

Einrichten des ESXi-Hosts zum Starten von iSCSI

Sie können ESXi-Hosts mithilfe des Software-iSCSI-Adapters oder eines abhängige Hardware-iSCSI-Adapters und eines Netzwerkadapters von iSCSI starten.

Wenn Sie Ihren Host für das Starten von iSCSI einrichten, führen Sie mehrere Aufgaben durch.

1 Konfigurieren der iSCSI-Startparameter auf Seite 74

Ein Netzwerkadapter auf Ihrem Host muss über eine speziell konfigurierte iSCSI-Start-Firmware verfügen, um den iSCSI-Startvorgang zu starten. Wenn Sie die Firmware konfigurieren, geben Sie die Netzwerk- und iSCSI-Parameter an und aktivieren Sie den Adapter für den iSCSI-Start.

2 Ändern der Startsequenz im BIOS auf Seite 74

Wenn Sie Ihren Host so einrichten, dass er vom iBFT-iSCSI gestartet wird, ändern Sie die Startsequenz, sodass Ihr Host in der entsprechenden Reihenfolge gestartet wird.

3 Installieren von ESXi auf dem iSCSI-Ziel auf Seite 75

Sie müssen beim Einrichten Ihres ESX-Hosts zum Starten von iSCSI das ESXi-Image auf der Ziel-LUN installieren.

4 Starten von ESXi vom iSCSI-Ziel auf Seite 75

Führen Sie nach dem Vorbereiten des Hosts für den iSCSI-Start und dem Kopieren des ESXi-Images auf das iSCSI-Ziel den eigentlichen Startvorgang aus.

Konfigurieren der iSCSI-Startparameter

Ein Netzwerkadapter auf Ihrem Host muss über eine speziell konfigurierte iSCSI-Start-Firmware verfügen, um den iSCSI-Startvorgang zu starten. Wenn Sie die Firmware konfigurieren, geben Sie die Netzwerk- und iSCSI-Parameter an und aktivieren Sie den Adapter für den iSCSI-Start.

Die Konfiguration auf dem Netzwerkadapter kann dynamisch oder statisch sein. Wenn Sie die dynamische Konfiguration verwenden, geben Sie an, dass alle Ziel- und Initiator-Startparameter über DHCP bezogen werden. Bei der statischen Konfiguration geben Sie Daten manuell ein, zu denen die IP-Adresse und der Initiator-IQN Ihres Hosts sowie die Zielparameter gehören.

Vorgehensweise

- Geben Sie auf dem Netzwerkadapter, den Sie zum Starten von iSCSI verwenden, die Netzwerk- und iSCSI-Parameter an.

  Da die Konfiguration des Netzwerkadapters herstellerabhängig ist, lesen Sie die Anweisungen in der Dokumentation Ihres Herstellers.

Ändern der Startsequenz im BIOS

Wenn Sie Ihren Host so einrichten, dass er vom iBFT-iSCSI gestartet wird, ändern Sie die Startsequenz, sodass Ihr Host in der entsprechenden Reihenfolge gestartet wird.

Ändern Sie für eine ESXi-Installation die BIOS-Startsequenz auf die folgende Sequenz:

- iSCSI
- DVD-ROM

Weil das Ändern der Startsequenz im BIOS herstellerspezifisch ist, sollten Sie die entsprechenden Anweisungen in der Herstellerdokumentation zu Rate ziehen. In der nachfolgenden Beispielprozedur wird veranschaulicht, wie die Startsequenz eines Dell-Hosts mit einem Broadcom-Netzwerkadapter geändert wird.

Vorgehensweise

1 Schalten Sie den Host ein.

2 Drücken Sie F2 während der Selbstdiagnose des Einschaltvorgangs (POST = Power-On Self-Test), um das BIOS-Setup aufzurufen.

3 Wählen Sie im BIOS-Setup **[Boot Sequence]** und drücken Sie die Eingabetaste.

4 Ordnen Sie im Startsequenz-Menü die startbaren Elemente so, dass iSCSI dem DVD-ROM voransteht.

5 Drücken Sie ESC, um das Startsequenz-Menü zu verlassen.

6 Durcken Sie die ESC-Taste, um das BIOS-Setup zu beenden.

7 Wählen Sie **[Änderungen speichern]** und klicken Sie auf **[Beenden]**, um das BIOS-Setup-Menü zu beenden.

Installieren von ESXi auf dem iSCSI-Ziel

Sie müssen beim Einrichten Ihres ESX-Hosts zum Starten von iSCSI das ESXi-Image auf der Ziel-LUN installieren.

Voraussetzungen

- Konfigurieren Sie die iSCSI-Start-Firmware auf Ihrer Start-Netzwerkkarte, um auf die Ziel-LUN zu verweisen, die Sie als Start-LUN verwenden möchten.
- Ändern Sie die Startsequenz im BIOS, sodass iSCSI dem DVD-Laufwerk vorangestellt wird.
- Falls Sie Broadcom-Adapter verwenden, legen Sie die Option **[Boot to iSCSI target]** auf **[Disabled]** fest

Vorgehensweise

1 Legen Sie das Installationsmedium in das DVD-ROM-Laufwerk ein und starten Sie den Host neu.

2 Wenn das Installationsprogramm startet, führen Sie die Standardinstallationsprozedur aus.

3 Wählen Sie die iSCSI-LUN als Installationsziel aus, wenn Sie dazu aufgefordert werden.

Das Installationsprogramm kopiert das ESXi-Start-Image in die iSCSI-LUN.

4 Entfernen Sie nach dem Neustart des Systems die Installations-DVD aus dem Laufwerk.

Starten von ESXi vom iSCSI-Ziel

Führen Sie nach dem Vorbereiten des Hosts für den iSCSI-Start und dem Kopieren des ESXi-Images auf das iSCSI-Ziel den eigentlichen Startvorgang aus.

Voraussetzungen

- Konfigurieren Sie die iSCSI-Start-Firmware auf Ihrer Start-Netzwerkkarte, um auf die Ziel-LUN zu verweisen.
- Ändern Sie die Startsequenz im BIOS, sodass iSCSI dem Startgerät vorangestellt wird.
- Falls Sie Broadcom-Adapter verwenden, legen Sie die Option **[Boot to iSCSI target]** auf **[Enabled]** fest

Vorgehensweise

1 Starten Sie den Host neu.

Der Host startet mithilfe von iBFT-Daten vom iSCSI-LUN. Beim Erststart richtet das iSCSI-Initialisierungsskript das Standardnetzwerk ein. Das Netzwerk-Setup überdauert nachfolgende Neustarts.

2 (Optional) Passen Sie die Netzwerkkonfiguration mithilfe des vSphere-Clients an.

Optimale Vorgehensweisen für Netzwerke

Sie müssen zum Starten eines ESXi-Hosts von iSCSI mithilfe von iBFT das Netzwerk ordnungsgemäß konfigurieren.

Für eine höhere Sicherheit und größere Leistung sollten auf dem Host redundante Netzwerkadapter vorhanden sein.

Wie Sie alle Netzwerkadapter einrichten, hängt davon ab, ob Ihre Umgebung für den iSCSI-Datenverkehr und den Hostverwaltungs-Datenverkehr freigegebene oder isolierte Netzwerke verwendet.

Freigegebene iSCSI- und Verwaltungsnetzwerke

Konfigurieren Sie die Netzwerk- und iSCSI-Parameter auf dem ersten Netzwerkadapter auf dem Host. Nach dem Starten des Hosts können Sie sekundäre Netzwerkadapter zur Standard-Portgruppe hinzufügen.

Isolierte iSCSI- und Verwaltungsnetzwerke

Befolgen Sie diese Richtlinien, wenn Sie isolierte iSCSI- und Verwaltungsnetzwerke konfigurieren.

- Ihre isolierten Netzwerke müssen sich in verschiedenen Subnetzen befinden.
- Wenn Sie zum Isolieren der Netzwerke VLANs verwenden, müssen diese verschiedene Subnetze haben, um die ordnungsgemäße Einrichtung der Routing-Tabellen sicherzustellen.
- Es wird empfohlen, die Konfiguration so vorzunehmen, dass sich der iSCSI-Adapter und das Ziel in demselben Subnetz befinden. Es gelten die folgenden Einschränkungen, wenn Sie den iSCSI-Adapter und das Ziel in unterschiedlichen Subnetzen einrichten:
  - Das Standard-VMkernel-Gateway muss in der Lage sein, sowohl den Verwaltungs- als auch den iSCSI-Datenverkehr weiterzuleiten.
  - Nachdem Sie Ihren ESXi-Host gestartet haben, können Sie den iBFT-aktivierten Netzwerkadapter nur für iBFT verwenden. Sie können den Adapter nicht für den iSCSI-Datenverkehr verwenden.
- Verwenden Sie den ersten physischen Netzwerkadapter für das Verwaltungsnetzwerk.
- Verwenden Sie den zweiten physischen Netzwerkadapter für das iSCSI-Netzwerk. Stellen Sie sicher, dass Sie die iBFT konfigurieren.
- Nach dem Starten des Hosts können Sie sekundäre Netzwerkadapter zu den Verwaltungs- und iSCSI-Netzwerken hinzufügen.

Ändern von iBFT-iSCSI-Starteinstellungen

Falls sich auf dem iSCSI-Speicher oder Ihrem Host Einstellungen ändern, wie z. B. der IQN-Name oder die IP-Adresse, aktualisieren Sie die iBFT. Für diese Aufgabe wird vorausgesetzt, dass die Start-LUN und die auf der LUN gespeicherten Daten intakt bleiben.

Vorgehensweise

1 Fahren Sie den ESXi-Host herunter.

2 Ändern Sie die iSCSI-Speichereinstellungen.

3 Aktualisieren Sie die iBFT auf dem Host mit den neuen Einstellungen.

4 Starten Sie den Host neu.

Der Host startet mit den neuen Informationen, die in der iBFT gespeichert sind.

iBFT-iSCSI-Start - Fehlerbehebung

In den Themen dieses Abschnitts wird beschrieben, wie Sie Probleme identifizieren und beheben, die beim Verwenden des iBFT-iSCSI-Startvorgangs auftreten können.

Verlust des Gateways des Systems verursacht einen Ausfall der Netzwerkverbindung

Die Netzwerkverbindung geht verloren, wenn Sie eine dem iBFT-Netzwerkadapter zugewiesene Portgruppe löschen.

Problem

Die Netzwerkverbindung geht nach dem Löschen einer Portgruppe verloren.

Ursache

Wenn Sie während der Installation von ESXi ein Gateway im iBFT-aktivierten Netzwerkadapter angeben, wird dieses Gateway zum Standard-Gateway des Systems. Das Standard-Gateway des Systems geht verloren, wenn Sie die dem Netzwerkadapter zugewiesene Portgruppe löschen. Diese Aktion verursacht den Verlust der Netzwerkverbindung.

Lösung

Legen Sie ein iBFT-Gateway daher nur dann fest, wenn es erforderlich ist. Wenn das Gateway erforderlich ist, legen Sie nach der Installation das Standard-Gateway des Systems auf das Gateway fest, das das Verwaltungsnetzwerk verwendet.

Ändern der iSCSI-Startparameter sorgt dafür, dass ESXi in statusfreiem Modus startet

Durch das Ändern der iSCSI-Startparameter auf dem Netzwerkadapter nach dem Erststart wird die iSCSI- und Netzwerkkonfiguration auf dem ESXi-Host nicht aktualisiert.

Problem

Wenn Sie nach dem ersten ESXi-Start von iSCSI die iSCSI-Startparameter auf dem Netzwerkadapter ändern, startet der Host in einem statusfreien Modus.

Ursache

Die Firmware verwendet die aktualisierte Startkonfiguration und kann eine Verbindung mit dem iSCSI-Ziel herstellen und das ESXi-Image laden. Wenn geladen, greift das System jedoch nicht auf die neuen Parameter zurück, sondern verwendet weiterhin die dauerhaften Netzwerk- und iSCSI-Parameter aus dem vorherigen Startvorgang. Infolgedessen kann der ESXi-Host keine Verbindung zum Ziel herstellen und startet im statusfreien Modus.

Lösung

1 Stellen Sie über den vSphere-Client eine Verbindung mit dem ESXi-Host her.

2 Konfigurieren Sie iSCSI und das Netzwerk auf dem Host neu, sodass sie mit den iBFT-Parametern übereinstimmen.

3 Führen Sie eine erneute Prüfung durch.

Erfassen von Diagnoseinformationen für ESXi-Hosts

Wenn Sie mithilfe von iBFT vom SAN starten und Ihr ESXi-Host über keine lokale Diagnosepartition verfügt, müssen Sie den vSphere Management Assistant (vMA) so einrichten, dass Diagnoseinformationen von Ihrem Host erfasst und für die anschließende Analyse gespeichert werden.

Falls schwerwiegende Probleme bei Ihrem ESXi-Host auftreten, erstellt Netz-Dump eine Datei mit Diagnoseinformationen, die anschließend analysiert werden können, um die Ursache des Problems festzustellen.

Richten Sie Ihren ESXi-Host so ein, dass er als Netz-Dump-Client agiert, der die Diagnosedatei über das Netzwerk überträgt. vMA dient als Netz-Dump-Server, der die Diagnoseinformationen erfasst und im Verzeichnis `/var/core` auf dem Server speichert.

Befolgen Sie diese Richtlinien, wenn Sie die Netz-Dump-Umgebung einrichten:

- Installieren Sie vMA nicht auf demselben physischen Host, auf dem Sie den Netz-Dump-Client eingerichtet haben.
- Wenn Sie mehrere ESXi-Hosts haben, die die Netz-Dump-Konfiguration benötigen, konfigurieren Sie jeden Host einzeln. Eine vMA-Instanz reicht aus, um die Core-Dump-Dateien von mehreren ESXi-Hosts zu erfassen.

Konfigurieren des vSphere Management Assistant

vSphere Management Assistant (vMA) ist eine virtuelle Maschine, die Sie zum Agieren als Netz-Dump-Server für das Erfassen von Diagnoseinformationen von Ihrem ESXi-Host konfigurieren.

Voraussetzungen

Stellen Sie vMA bereit und konfigurieren Sie ihn auf einem physischen Server, der sich von dem Server unterscheidet, auf dem Sie den Netz-Dump-Client eingerichtet haben. Weitere Informationen finden Sie im *vSphere Management Assistant Guide* auf http://www.vmware.com/support/pubs.

Vorgehensweise

1 Melden Sie sich bei vMA als Administrator an.

2 Aktivieren Sie den Netz-Dump-Server auf vMA.

```
# sudo chkconfig vmware-netdumper on
```

3 Starten Sie den Netz-Dump-Server.

```
# sudo/etc/init.d/vmware-netdumper start
```

```
# sudo lokkit --quiet --port=6500:udp
```

Konfigurieren des ESXi-Hosts

Konfigurieren Sie einen ESXi-Host, sodass er als der Netz-Dump-Client agiert, der Diagnoseinformationen über das Netzwerk überträgt.

Verwenden Sie die vSphere-CLI zum Konfigurieren des ESXi-Hosts.

Voraussetzungen

Konfigurieren Sie vMA als den Netz-Dump-Server und beziehen Sie dessen IP-Adresse.

Vorgehensweise

1 Geben Sie die IP-Adresse des ESXi-Hosts ein.

```
# esxcfg-advcfg -s IP_address_ESXi /Net/NetdumpVmkIP
```

2 Geben Sie den zu verwendenden Netzwerkadapter an.

```
# esxcfg-advcfg -s vmnic /Net/NetdumpVmkNic
```

3 Geben Sie die Portgruppe an, die mit dem Netzwerkadapter verbunden ist.

```
# esxcfg-advcfg -s Portgruppe /Net/NetdumpVmkPG
```

4 Geben Sie die IP-Adresse des Netz-Dump-Servers an.

```
# esxcfg-advcfg -s IP_address_netdump /Net/NetdumpServerIP
```

5 (Optional) Geben Sie die IP-Adresse des Gateways zum Erreichen des Netz-Dump-Servers ein.

```
# esxcfg-advcfg -s IP_address_gateway /Net/NetdumpServerGateway
```

Verwalten von ESX/ESXi-Systemen, die einen SAN-Speicher verwenden 5

In diesem Abschnitt erfahren Sie, wie Sie Ihr ESX/ESXi-System verwalten, SAN-Speicher effektiv verwenden und Fehlerbehebung durchführen. Außerdem wird erklärt, wie Sie Informationen zu Speichergeräten, Adaptern, Multipathing usw. abrufen können.

Dieses Kapitel behandelt die folgenden Themen:

- „Anzeigen von Informationen zu Speicheradaptern“, auf Seite 79
- „Anzeigen von Informationen zu Speichergeräten“, auf Seite 80
- „Anzeigen von Datenspeicherinformationen“, auf Seite 83
- „Beheben von Problemen bei der Speicheranzeige“, auf Seite 84
- „Prüfen und Beanspruchen von Pfaden“, auf Seite 89
- „Gemeinsame Nutzung von Diagnosepartitionen“, auf Seite 94
- „Vermeiden und Beheben von SAN-Problemen“, auf Seite 95
- „Optimieren der SAN-Speicherleistung“, auf Seite 95
- „Beheben von Leistungsproblemen“, auf Seite 99
- „Überlegungen zu SAN-Speichersicherungen“, auf Seite 103
- „Verwalten von duplizierten VMFS-Datenspeichern“, auf Seite 105
- „Speicherhardware-Beschleunigung“, auf Seite 108

Anzeigen von Informationen zu Speicheradaptern

Im vSphere-Client können Sie die von Ihrem Host verwendeten Speicheradapter anzeigen lassen und ihre Informationen überprüfen.

Wenn Sie alle verfügbaren Speicheradapter auflisten, können Sie ihr Modell, ihren Typ, z. B. Fibre-Channel, Paralleles SCSI oder iSCSI, und, falls verfügbar, ihre eindeutigen Bezeichner anzeigen.

Als eindeutige Bezeichner verwenden iSCSI-Adapter iSCSI-Namen.

Beim Abrufen von Details für jeden einzelnen iSCSI-Adapter werden die folgenden Informationen angezeigt. Software-iSCSI- und abhängige Hardware-iSCSI-Adapter müssen konfiguriert oder aktiviert werden, bevor Sie deren Informationen ansehen können.

Tabelle 5-1. Informationen zu Speicheradaptern

Adapterinformationen	Beschreibung
Modell	Adaptermodell.
iSCSI-Name	Ein in Übereinstimmung mit den iSCSI-Standards erstellter eindeutiger Name, der den FC-Adapter eindeutig identifiziert.
iSCSI-Alias	Ein benutzerfreundlicher Name, der anstelle des iSCSI-Namens verwendet wird.
IP-Adresse (unabhängige Hardware-iSCSI)	Eine dem iSCSI-Adapter zugewiesene Adresse.
Verbundene Ziele	Die Anzahl der Ziele, auf die über den Adapter zugegriffen wurde.
Geräte	Alle Speichergeräte oder LUNs, auf die der Adapter zugreifen kann.
Pfade	Alle vom Adapter zum Zugreifen auf Speichergeräte verwendeten Pfade.

Anzeigen von Informationen zu Speicheradaptern

Verwenden Sie den vSphere-Client, um Speicheradapter sowie die dazugehörigen Informationen anzuzeigen.

Vorgehensweise

1 Wählen Sie **[Hosts und Cluster]** in der Bestandsliste aus.

2 Wählen Sie einen Host und klicken Sie auf die Registerkarte **[Konfiguration]** .

3 Wählen Sie **[Speicheradapter]** im Fenster „Hardware“ aus.

4 Wählen Sie einen Adapter in der Liste „Speicheradapter“ aus, um Details dazu anzeigen zu lassen.

5 Klicken Sie zum Auflisten aller Speichergeräte, auf die der Adapter zugreifen kann, auf **[Geräte]** .

6 Klicken Sie zum Auflisten aller Pfade, die der Adapter verwendet, auf **[Pfade]** .

Kopieren von Speicheradapternamen in die Zwischenablage

Sie können den Namen eines Adapters dirket aus der Benutzerschnittstelle in die Zwischenablage kopieren.

Vorgehensweise

1 Wählen Sie **[Hosts und Cluster]** in der Bestandsliste aus.

2 Wählen Sie einen Host und klicken Sie auf die Registerkarte **[Konfiguration]** .

3 Wählen Sie **[Speicheradapter]** im Fenster „Hardware“ aus.

4 Wählen Sie den Adapter in der Liste „Speicheradapter“ aus.

5 Markieren Sie im Fenster „Details“ den Wert im Namensfeld und wählen Sie **[Kopieren]** aus dem Kontextmenü aus.

Anzeigen von Informationen zu Speichergeräten

Sie können im vSphere-Client alle für Ihren Host verfügbaren Speichergeräte oder LUNs anzeigen, einschließlich aller lokalen Geräte und Netzwerkgeräte. Wenn Sie Multipathing-Plug-Ins von Drittanbietern verwenden, werden durch die Plug-Ins verfügbare Speichergeräte ebenfalls in der Liste angezeigt.

Sie können für jeden Speicheradapter eine Liste von Speichergeräten anzeigen, die nur über diesen Adapter verfügbar sind. In der Regel wird Ihnen beim Überprüfen einer Liste von Speichergeräten Folgendes angezeigt.

Tabelle 5-2. Informationen zum Speichergerät

Geräteinformationen	Beschreibung
Name	Ein benutzerfreundlicher Name, den der Host einem Gerät anhand des Speichertyps und Herstellers zuweist. Sie können diesen Namen ändern.
Bezeichner	Eine für ein bestimmtes Speichergerät spezifische UUID.
Laufzeitname	Der Name des ersten Pfads zum Gerät.
LUN	Die LUN-Nummer, die die Position der LUN innerhalb des Ziels anzeigt.
Typ	Gerätetyp, z. B. Festplatte oder CD-ROM-Laufwerk.
Transport	Das Transportprotokoll, das Ihr Host für den Zugriff auf das Gerät verwendet.
Kapazität	Gesamtkapazität des Speichergeräts.
Besitzer	Das vom Host zum Verwalten des Speichergeräts verwendete Plug-In, z. B. das NMP oder ein Drittanbieter-Plug-In.
Hardwarebeschleunigung	Informationen dazu, ob das Speichergerät den Host bei verschiedenen Vorgängen für die Verwaltung virtueller Maschinen unterstützt. Der Status kann „Unterstützt“, „Nicht unterstützt“ oder „Unbekannt“ lauten.
Speicherort	Ein Pfad zum Speichergerät im Verzeichnis `/vmfs/devices/`.
Partitionen	Primäre und logische Partitionen, einschließlich eines VMFS-Datenspeichers, sofern konfiguriert.

Grundlegendes zur Benennung von Speichergeräten

Im vSphere-Client wird jedes Speichergerät bzw. jede LUN durch mehrere Namen identifiziert.

Name Ein benutzerfreundlicher Name, den der Host einem Gerät anhand des Speichertyps und Herstellers zuweist. Sie können den Namen über den vSphere-Client ändern.

Bezeichner Eine UUID, die der Host aus dem Speicher extrahiert. Je nach Speichertyp verwendet der Host unterschiedliche Algorithmen zum Extrahieren des Bezeichners.

Laufzeitname Der Name des ersten Pfads zum Gerät. Der Laufzeitname wird vom Host erstellt. Der Laufzeitname ist kein zuverlässiger Bezeichner für das Gerät und ist nicht dauerhaft.

Die Laufzeitname hat das folgende Format:

vmhba#:C#:T#:L#, wobei

- „vmhba#“ der Name des Speicheradapters ist. Der Name bezieht sich auf den physischen Adapter auf dem Host, nicht auf den SCSI-Controller, den die virtuellen Maschinen verwenden.
- C# ist die Nummer des Speicherkanals.

  Software-iSCSI-Initiatoren verwenden die Nummer des Speicherkanals, um mehrere Pfade zu demselben Ziel anzuzeigen.

- T# ist die Zielnummer. Die Zielnummerierung wird vom Host entschieden und kann sich ändern, wenn es eine Änderung in der Zuordnung von Zielen gibt, die für den Host sichtbar sind. Von verschiedenen Hosts gemeinsam verwendete Ziele verfügen möglicherweise nicht über dieselbe Zielnummer.
- L# ist die LUN-Nummer, die die Position der LUN innerhalb des Ziels anzeigt. Die LUN-Nummer wird vom Speichersystem bereitgestellt. Wenn ein Ziel nur über eine LUN verfügt, ist die LUN-Nummer immer Null (0).

Beispielsweise repräsentiert `vmhba1:C0:T3:L1` LUN1 auf Ziel 3, auf die über den Speicheradapter vmhba1 und den Kanal 0 zugegriffen wird.

Anzeigen von Speichergeräten für einen Host

Sie können im vSphere-Client alle für Ihren Host verfügbaren Speichergeräte oder LUNs anzeigen, einschließlich aller lokalen Geräte und Netzwerkgeräte. Wenn Sie Multipathing-Plug-Ins von Drittanbietern verwenden, werden durch die Plug-Ins verfügbare Speichergeräte ebenfalls in der Liste angezeigt.

Vorgehensweise

1 Wählen Sie **[Hosts und Cluster]** in der Bestandsliste aus.

2 Wählen Sie einen Host und klicken Sie auf die Registerkarte **[Konfiguration]** .

3 Klicken Sie unter „Hardware“ auf **[Speicher]** .

4 Klicken Sie auf **[Geräte]** .

5 Wählen Sie ein Gerät in der Liste aus, wenn Sie zusätzlich Details zu diesem bestimmten Gerät erfahren möchten.

Anzeigen von Speichergeräten für einen Adapter

Sie können für jeden Speicheradapter auf Ihrem Host eine Liste von Speichergeräten anzeigen, die nur über diesen Adapter verfügbar sind.

Vorgehensweise

1 Wählen Sie **[Hosts und Cluster]** in der Bestandsliste aus.

2 Wählen Sie einen Host und klicken Sie auf die Registerkarte **[Konfiguration]** .

3 Wählen Sie **[Speicheradapter]** im Fenster „Hardware“ aus.

4 Wählen Sie den Adapter in der Liste „Speicheradapter“ aus.

5 Klicken Sie auf **[Geräte]** .

Kopieren von Speichergerätebezeichnern in die Zwischenablage

Ein Speichergerätebezeichner ist eine UUID, die der Host einem Speichergerät oder einer LUN zuweist. Je nach Speichertyp verwendet der Host unterschiedliche Algorithmen zum Erstellen des Bezeichners, der ziemlich lang und komplex werden kann. Sie können den Speichergerätebezeichner direkt aus der Benutzerschnittstelle kopieren.

Vorgehensweise

1 Zeigen Sie eine Liste von Speichergeräten an.

2 Klicken Sie mit der rechten Maustaste auf ein Gerät und wählen Sie **[Bezeichner in die Zwischenablage kopieren]** .

Anzeigen von Datenspeicherinformationen

Sie können alle auf den Hosts verfügbaren Datenspeicher anzeigen und deren Eigenschaften analysieren.

Es gibt folgende Möglichkeiten, dem vSphere-Client Datenspeicher hinzufügen:

- Erstellung auf einem verfügbaren Speichergerät.
- Erkennung, sobald ein Host der Bestandsliste hinzugefügt wird. Wenn Sie der Bestandsliste einen Host hinzufügen, zeigt der vSphere-Client alle Datenspeicher an, die dem Host zur Verfügung stehen.

Wenn Ihr vSphere-Client mit einem vCenter Server-System verbunden ist, können Sie die Datenspeicherinformationen in der Ansicht „Datenspeicher“ anzeigen. In dieser Ansicht werden alle Datenspeicher in der Bestandsliste nach Datencenter sortiert angezeigt. Mithilfe dieser Ansicht können Sie Datenspeicher in Ordnerhierarchien organisieren, neue Datenspeicher erstellen, ihre Eigenschaften bearbeiten und vorhandene Datenspeicher entfernen.

Diese Ansicht zeigt umfangreiche Informationen zu Ihren Datenspeichern an. Dazu gehören die Hosts und die virtuellen Maschinen, die die Datenspeicher verwenden, Informationen zu Speicherberichten, Berechtigungen, Alarme, Aufgaben und Ereignisse, die Speichertopologie sowie die Speicherberichte selbst. Für jeden Datenspeicher werden auf der Registerkarte „Konfiguration“ in der Ansicht „Datenspeicher“ Konfigurationsinformationen zu allen mit dem Datenspeicher verbundenen Hosts aufgeführt.

Hinweis Die Ansicht „Datenspeicher“ ist nicht verfügbar, wenn der vSphere-Client direkt mit Ihrem Host verbunden ist. In diesem Fall können Sie über die Registerkarte für die hostspezifische Speicherkonfiguration Datenspeicherinformationen einsehen.

In der folgenden Tabelle werden die Datenspeicherdetails aufgeführt, die Ihnen beim Prüfen von Datenspeichern angezeigt werden.

Tabelle 5-3. Informationen zu Datenspeichern

Informationen zu Datenspeichern	Beschreibung
Identifikation	Bearbeitbarer, benutzerfreundlicher Name, den Sie dem Datenspeicher zuweisen können.
Gerät	Speichergerät, auf dem der Datenspeicher bereitgestellt wird. Wenn sich der Datenspeicher über mehrere Speichergeräte erstreckt, wird nur das erste Speichergerät angezeigt.
Kapazität	Formatierte Gesamtkapazität des Datenspeichers.
Frei	Verfügbarer Speicherplatz.
Typ	Dateisystem, das der Datenspeicher verwendet, entweder VMFS oder NFS.
Speicher-E/A-Steuerung	Ermöglicht die clusterweite Speicher-E/A-Priorisierung. Weitere Informationen finden Sie im *Handbuch zur vSphere-Ressourcenverwaltung*.

Tabelle 5-3. Informationen zu Datenspeichern (Fortsetzung)

Informationen zu Datenspeichern	Beschreibung
Hardwarebeschleunigung	Informationen dazu, ob der Datenspeicher den Host bei verschiedenen Vorgängen für die Verwaltung virtueller Maschinen unterstützt. Der Status kann „Unterstützt“, „Nicht unterstützt“ oder „Unbekannt“ lauten.
Speicherort	Ein Pfad zum Datenspeicher im Verzeichnis `/vmfs/volumes/`.
Erweiterungen	Einzelne Erweiterungen, aus denen der Datenspeicher besteht, samt Kapazität (nur VMFS-Datenspeicher).
Pfadauswahl	Pfadauswahlrichtlinie, die der Host zum Zugriff auf den Speicher verwendet (nur VMFS-Datenspeicher).
Pfade	Anzahl der Pfade, die zum Zugriff auf den Speicher verwendet werden, und deren Status (nur VMFS-Datenspeicher).

Überprüfen von Datenspeichereigenschaften

Verwenden Sie den vSphere-Client, um die Datenspeichereigenschaften zu überprüfen.

Vorgehensweise

1 Wählen Sie in der Bestandsliste einen Host aus und klicken Sie auf die Registerkarte **[Konfiguration]** .

2 Klicken Sie unter „Hardware“ auf **[Speicher]** .

3 Klicken Sie unter „Ansicht“ auf **[Datenspeicher]** .

4 Wählen Sie einen Datenspeicher in der Liste aus, um Details dazu anzuzeigen.

Beheben von Problemen bei der Speicheranzeige

Wenn Sie den vSphere-Client zum Anzeigen von auf Ihrem ESX/ESXi-Host verfügbaren Speichergeräten verwenden und der Host nicht Ihren Erwartungen entspricht, führen Sie die folgenden Fehlerbehebungsaufgabe durch.

Führen Sie bei Anzeigeproblemen die folgenden Fehlerbehebungsaufgabe durch.

Tabelle 5-4. Fehlerbehebung bei der iSCSI-LUN-Anzeige

Fehlerbehebungsaufgabe	Beschreibung
Prüfen Sie die Kabelverbindung.	Wenn ein Port nicht angezeigt wird, ist die Ursache dieses Problems möglicherweise die Kabelverbindung oder das Routing. Überprüfen Sie zunächst die Kabel. Stellen Sie sicher, dass die Ports mit Kabeln verbunden sind und eine Leuchte anzeigt, dass die Verbindung ordnungsgemäß funktioniert. Wenn dies nicht an beiden Enden des Kabels der Fall ist, ersetzen Sie das Kabel.
Prüfen Sie die Routing-Einstellungen.	Steuert die Konnektivität zwischen verschiedenen Subnetzen in Ihrer Ethernet-Konfiguration. Wenn sich das ESX/ESXi-System und der iSCSI-Speicher nicht in demselben Subnetz befinden, stellen Sie sicher, dass das Routing zwischen den Subnetzen ordnungsgemäß funktioniert. Stellen Sie ferner sicher, dass die Subnetzmaske und Gateway-Adresse im iSCSI-Speicher und iSCSI-Initiator auf dem ESX/ESXi-Host ordnungsgemäß konfiguriert sind.

Tabelle 5-4. Fehlerbehebung bei der iSCSI-LUN-Anzeige (Fortsetzung)

Fehlerbehebungsaufgabe	Beschreibung
Prüfen Sie die Konfiguration der Zugriffssteuerung.	Wenn die erwarteten LUNs nach dem erneuten Überprüfen nicht angezeigt werden, ist die Zugriffssteuerung auf Speichersystemseite möglicherweise nicht ordnungsgemäß konfiguriert. ■ Wenn CHAP konfiguriert ist, stellen Sie sicher, dass das Protokoll auf dem ESX/ESXi-Host aktiviert ist und der Einrichtung des Speichersystems entspricht. ■ Wenn die IP-basierte Filterung verwendet wird, stellen Sie sicher, dass die IP-Adresse von iSCSI-HBA oder VMkernel-Portgruppe sowie die IP-Adresse der Servicekonsole zulässig sind. ■ Wenn Sie die auf dem Initiator-Namen basierende Filterung verwenden, stellen Sie sicher, dass der Name ein qualifizierter iSCSI-Name ist und der Einrichtung des Speichersystems entspricht. ■ Um über ein SAN zu starten, stellen Sie sicher, dass jedem Host ausschließlich die erforderlichen LUNs angezeigt werden. Legen Sie fest, dass für einen Host keine Start-LUNs mit Ausnahme der eigenen sichtbar sind. Verwenden Sie Speichersystemsoftware, um sicherzustellen, dass dem Host ausschließlich die erforderlichen LUNs angezeigt werden. ■ Stellen Sie sicher, dass die Einstellung **[Disk.MaxLUN]** das Anzeigen der erwarteten LUN zulässt.
Prüfen Sie die Einrichtung der Speicherprozessoren.	Wenn ein Speicherprozessor über mehrere Speicherprozessoren verfügt, stellen Sie sicher, dass der SAN-Switch mit dem Speicherprozessor verbunden ist, dem die LUNs zugewiesen sind, auf die Sie zugreifen möchten. In einigen Speichersystemen ist lediglich ein Speicherprozessor aktiv, und die anderen Speicherprozessoren sind so lange passiv, bis ein Failover eintritt. Wenn Sie mit dem falschen Speicherprozessor verbunden sind (dem mit dem passiven Pfad), werden die erwarteten LUNs möglicherweise nicht angezeigt, oder die LUNs werden angezeigt, beim Versuch, darauf zuzugreifen, erhalten Sie jedoch Fehlermeldungen.
Prüfen Sie für iSCSI die Netzwerkkonfiguration.	Der Software-iSCSI-Initiator in ESX/ESXi erfordert, dass ein VMkernel-Netzwerkport auf den iSCSI-Speicher zugreifen kann. Der Software-Initiator verwendet den VMkernel für die Datenübertragung zwischen dem ESX/ESXi-System und dem iSCSI-Speicher.
Prüfen Sie den iSCSI-Initiator erneut.	Führen Sie eine erneute Prüfung durch, wenn Sie eine der folgenden Aufgaben ausgeführt haben: ■ Erstellen von neuen LUNs in einem SAN. ■ Ändern der LUN-Maskierung in einem ESX/ESXi-Hostspeichersystem. ■ Erneutes Verbinden eines Kabels. ■ Ändern eines Hosts in einem Cluster ■ Ändern der CHAP-Einstellungen oder Hinzufügen neuer Erkennungsadressen.

Vorgänge zum Aktualisieren des Datenspeichers und erneuten Prüfen des Speichers

Der Vorgang zum Aktualisieren des Datenspeichers aktualisiert die Datenspeicherlisten und die Speicherinformationen, z. B. die Datenspeicherkapazität, die im vSphere-Client angezeigt werden. Wenn Sie Datenspeichermanagementaufgaben durchführen oder Änderungen an der SAN-Konfiguration vornehmen, müssen Sie möglicherweise Ihren Speicher erneut prüfen.

Wenn Sie VMFS-Datenspeicherverwaltungsvorgänge ausführen, z. B. das Erstellen eines VMFS-Datenspeichers oder RDMs, das Hinzufügen einer Erweiterung und das Vergrößern oder Löschen eines VMFS-Datenspeichers, wird Ihr Speicher von Ihrem Host oder dem vCenter Server automatisch neu geprüft und aktualisiert. Sie können die Funktion für die automatische Neuprüfung deaktivieren, indem Sie den Filter für das erneute Prüfen eines Hosts ausschalten. Weitere Informationen hierzu finden Sie unter „Ausschalten von vCenter Server-Speicherfiltern“, auf Seite 87.

In bestimmten Fällen müssen Sie die erneute Prüfung manuell durchführen. Sie können erneut alle verfügbaren Speicher Ihres Hosts prüfen oder, wenn Sie den vCenter Server einsetzen, alle Hosts in einem Ordner, Cluster und Datencenter.

Wenn sich die von Ihnen vorgenommenen Änderungen auf Speicher beschränken, die über einen bestimmten Adapter verbunden sind, führen Sie eine erneute Prüfung dieses Adapters durch.

Führen Sie eine erneute manuelle Prüfung durch, wenn Sie eine der folgenden Änderungen vorgenommen haben.

- Erstellen von neuen LUNs in einem SAN.
- Ändern Sie die Pfadmaskierung auf einem Host.
- Erneutes Verbinden eines Kabels.
- Ändern der CHAP-Einstellungen.
- Hinzufügen oder Entfernen von Erkennungsadressen oder statischen Adressen.
- Hinzufügen eines einzelnen Hosts zum vCenter Server, nachdem Sie einen Datenspeicher, der von den vCenter Server-Hosts und dem einzelnen Host gemeinsam genutzt wird, bearbeitet oder vom vCenter Server entfernt haben.

WICHTIG Wenn bei einer erneuten Prüfung kein Pfad verfügbar ist, entfernt der Host den Pfad aus der Liste der Pfade zu dem Gerät. Der Pfad wird erneut in der Liste angezeigt, sobald er verfügbar und wieder einsatzbereit ist.

Durchführen einer erneuten Speicherprüfung

Wenn Sie Änderungen an Ihrer Host- oder SAN-Konfiguration vornehmen, müssen Sie möglicherweise Ihren Speicher erneut prüfen. Sie können alle Speicher erneut prüfen, die Ihrem Host zur Verfügung stehen. Wenn sich die von Ihnen vorgenommenen Änderungen auf Speicher beschränken, auf die über einen bestimmten Adapter zugegriffen wird, führen Sie eine erneute Prüfung nur dieses Adapters durch.

Führen Sie die folgenden Schritte aus, wenn Sie die erneute Prüfung des Speichers, der einem bestimmten Host zur Verfügung steht oder auf den über einen bestimmten Adapter auf den Host zugegriffen wird, beschränken möchten. Wenn Sie den Speicher, der allen Hosts zur Verfügung steht, die von Ihrem vCenter Server-System verwaltetet werden, erneut prüfen möchten, können Sie dies tun, indem Sie mit der rechten Maustaste auf ein Datencenter, einen Cluster oder einen Ordner klicken, in dem sich die Hosts befinden, und die Option **[Erneut auf Datenspeicher prüfen]** wählen.

Vorgehensweise

1 Wählen Sie im vSphere-Client einen Host und klicken Sie auf die Registerkarte **[Konfiguration]** .

2 Wählen Sie im Fenster Hardware die Option **[Speicheradapter]** , und klicken Sie oberhalb des Fensters Speicheradapter auf **[Erneut prüfen]** .

Sie können auch mit der rechten Maustaste auf einzelne Adapter klicken und auf **[Erneut prüfen (Rescan)]** klicken, wenn Sie nur diesen Adapter erneut prüfen möchten.

WICHTIG Auf ESXi ist es nicht möglich, einen einzelnen Speicheradapter erneut zu prüfen. Wenn Sie eine erneute Prüfung für einen einzelnen Adapter durchführen, werden alle Adapter erneut geprüft.

3 Wenn neue Festplatten oder LUNs erkannt werden sollen, aktivieren Sie **[Auf neue Speichergeräte prüfen]** .

Wenn neue LUNs erkannt werden, werden sie in der Geräteliste angezeigt.

4 Um neue Datenspeicher zu erkennen oder einen Dateispeicher nach einer Konfigurationsänderung zu aktualisieren, wählen Sie **[Auf neue VMFS-Volumes prüfen (Scan for New VMFS Volumes)]** aus.

Wenn neue Datenspeicher oder VMFS-Datenträger erkannt werden, werden diese in der Datenspeicherliste angezeigt.

Ändern der Anzahl an LUNs, nach denen gesucht wird

Der VMkernel prüft standardmäßig auf LUN 0 bis LUN 255 für jedes Ziel (insgesamt 256 LUNs). Sie können den Parameter **[Disk.MaxLUN]** ändern, um die LUN-Erkennungsgeschwindigkeit zu verbessern.

WICHTIG LUNs mit einer höheren LUN-ID als 255 können nicht erkannt werden.

Durch das Verringern des Wertes kann die Zeit zum erneuten Prüfen und Starten verkürzt werden. Zeit zum erneuten Prüfen von LUNs hängt jedoch von verschiedenen Faktoren ab, u. a. davon, welcher Typ von Speichersystem verwendet wird und ob Unterstützung für Sparse-LUNs aktiviert ist.

Vorgehensweise

1. Wählen Sie im Bestandslistenbereich des vSphere-Clients den Host, klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend unter „Software“ auf **[Erweiterte Einstellungen]** .
2. Wählen Sie **[Festplatte]** .
3. Führen Sie einen Bildlauf zu **[Disk.MaxLUN]** durch.
4. Ändern Sie den vorhandenen Wert in einen Wert Ihrer Wahl und klicken Sie auf **[OK]** .

   Der eingegebene Wert gibt die LUn nach der letzten LUN an, die Sie suchen möchten.

   Wenn Sie beispielsweise nach LUNs von 0 bis 31 suchen möchten, setzten Sie **[Disk.MaxLUN]** auf 32.

Deaktivieren der Unterstützung für Sparse-LUNs

Sie können die standardmäßige Unterstützung für Sparse-LUNs deaktivieren, um die für ESX/ESXi erforderliche Zeit für die Suche nach LUNs zu reduzieren.

Der VMkernel ist standardmäßig für die Unterstützung von Sparse-LUNs konfiguriert. Die Unterstützung für Sparse-LUNs aktiviert den VMkernel zur Durchführung einer ununterbrochenen LUN-Suche, wenn ein Speichergerät LUNs mit einer willkürlichen LUN-Nummerierung darstellt, zum Beispiel 0, 6, und 23. Wenn alle LUNs Ihres Speichersystems nacheinander dargestellt werden, kann die Unterstützung für Sparse-LUNs deaktiviert werden.

Vorgehensweise

1. Wählen Sie im Bestandslistenbereich des vSphere-Clients den Host, klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend unter „Software“ auf **[Erweiterte Einstellungen]** .
2. Wählen Sie im Dialogfeld **[Erweiterte Einstellungen (Advanced Settings)]** die Option **[Festplatte]** .
3. Führen Sie einen Bildlauf zu **[Disk.SupportSparseLUN]** durch, ändern Sie den Wert in 0 und klicken Sie auf **[OK]** .

Ausschalten von vCenter Server-Speicherfiltern

Wenn Sie VMFS-Datenspeicherverwaltungsvorgänge ausführen, verwendet vCenter Server Standardspeicherfilter. Die Filter helfen Ihnen dadurch, Speicherschäden zu vermeiden, indem nur die Speichergeräte oder LUNs abgerufen werden, die für einen bestimmten Vorgang verwendet werden können. Ungeeignete LUNs werden nicht zur Auswahl angezeigt. Sie können die Filter ausschalten, um alle LUNs anzuzeigen.

Wenden Sie sich an den VMware-Support, bevor Sie Änderungen an den LUN-Filtern vornehmen. Sie können die Filter nur dann ausschalten, wenn Sie über andere Methoden zum Verhindern von LUN-Beschädigungen verfügen.

Vorgehensweise

1 Wählen Sie im vSphere-Client **[Verwaltung] > [vCenter Server-Einstellungen]** .

2 Wählen Sie in der Liste „Einstellungen“ den Eintrag **[Erweiterte Einstellungen]** aus.

3 Geben Sie einen Schlüssel im Feld **[Schlüssel]** ein.

Taste	Filtername
config.vpxd.filter.vmfsFilter	VMFS-Filter
config.vpxd.filter.rdmFilter	RDM-Filter
config.vpxd.filter.SameHostAndTransportsFilter	Filter für denselben Host und dieselben Transports
config.vpxd.filter.hostRescanFilter	Filter für das erneute Prüfen eines Hosts **Hinweis** Wenn Sie den Filter für das erneute Prüfen eines Hosts deaktivieren, führen Ihre Hosts weiterhin eine erneute Prüfung durch, sobald Sie für einen Host oder Cluster eine neue LUN bereitstellen.

4 Geben Sie im Textfeld **[Wert]** für den angegebenen Schlüssel `False` ein.

5 Klicken Sie auf **[Hinzufügen]** .

6 Klicken Sie auf **[OK]** .

Es ist nicht erforderlich, dass Sie das vCenter Server-System neu starten.

Filtern von vCenter Server-Speichern

vCenter Server bietet Speicherfilter, die Ihnen helfen, die Beschädigung von Speichergeräten oder das Nachlassen der Leistung zu vermeiden, die durch eine nicht unterstützte Nutzung von LUNs verursacht wird. Diese Filter stehen standardmäßig zur Verfügung.

Tabelle 5-5. Speicherfilter

Filtername	Beschreibung	Taste
VMFS-Filter	Filtert Speichergeräte oder LUNs, die bereits von einem VMFS-Datenspeicher auf einem von vCenter Server verwalteten Host verwendet werden. Die LUNs werden nicht als Kandidaten ausgewiesen, die mit einem anderen VMFS-Datenspeicher formatiert oder als RDM verwendet werden.	config.vpxd.filter.vmfsFilter
RDM-Filter	Filtert LUNs, die bereits von einem RDM auf einem von vCenter Server verwalteten Host verwendet werden. Die LUNs werden nicht als Kandidaten ausgewiesen, die mit VMFS formatiert oder von einem anderen RDM verwendet werden. Wenn virtuelle Maschinen auf dasselbe LUN zugreifen müssen, müssen sie dieselbe RDM-Zuordnungsdatei gemeinsam nutzen. Weitere Informationen über diesen Konfigurationstyp finden Sie unter *Setup für das Failover-Clustering und Microsoft Cluster Service*.	config.vpxd.filter.rdmFilter

Tabelle 5-5. Speicherfilter (Fortsetzung)

Filtername	Beschreibung	Taste
Filter für denselben Host und dieselben Transports	Filtert LUNs, die aufgrund der Inkompatibilität des Hosts oder des Speichertyps für die Verwendung als VMFS-Datenspeichererweiterungen ungeeignet sind. Verhindert, dass Sie die folgenden LUNs als Erweiterungen hinzufügen: ■ LUNs, die nicht für alle Hosts freigelegt sind, die den ursprünglichen VMFS-Datenspeicher gemeinsam nutzen. ■ LUNs, die einen Speichertyp verwenden, der sich vom Speichertyp des ursprünglichen VMFS-Datenspeichers unterscheidet. Sie können beispielsweise keine Fibre-Channel-Erweiterung zu einem VMFS-Datenspeicher auf einem lokalen Speichergerät hinzufügen.	config.vpxd.filter.SameHostAndTransportsFilter
Filter für das erneute Prüfen eines Hosts	Prüft VMFS-Datenspeicher automatisch neu und aktualisiert sie, nachdem Sie Datenspeicherverwaltungsvorgänge durchgeführt haben. Der Filter trägt dazu bei, eine konsistente Ansicht aller VMFS-Datenspeicher auf allen von vCenter Server verwalteten Hosts aufrechtzuerhalten. **Hinweis** Wenn Sie für einen Host oder Cluster eine neue LUN bereitstellen, führen die Hosts automatisch eine erneute Prüfung durch, unabhängig davon, ob der Filter für das erneute Prüfen eines Hosts aktiviert oder deaktiviert ist.	config.vpxd.filter.hostRescanFilter

Prüfen und Beanspruchen von Pfaden

Wenn Sie Ihren ESX/ESXi-Host starten oder Ihren Speicheradapter erneut prüfen, ermittelt der Host alle physischen Pfade zu Speichergeräten, die für den Host verfügbar sind. Auf Basis von Beanspruchungsregeln, die in der Datei `/etc/vmware/esx.conf` definiert sind, ermittelt der Host, welches Multipathing-Plug-In (MPP) die Pfade zu einem bestimmten Gerät beanspruchen und die Verwaltung der Multipathing-Unterstützung für das Gerät übernehmen soll.

Standardmäßig führt der Host alle 5 Minuten eine periodische Pfadauswertung durch, wodurch alle freien Pfade durch das entsprechende MPP beansprucht werden.

Die Beanspruchungsregeln sind nummeriert. Für jeden physischen Pfad arbeitet der Host die Beanspruchungsregeln ab und beginnt dabei mit der niedrigsten Nummer. Die Attribute des physischen Pfads werden mit der Pfadspezifikation in der Beanspruchungsregel verglichen. Wenn eine Übereinstimmung gefunden wird, weist der Host das in der Beanspruchungsregel angegebene MPP zum Verwalten des physischen Pfads zu. Dies wird so lange fortgesetzt, bis alle physischen Pfade durch entsprechende MPPs beansprucht werden, bei denen es sich um Drittanbieter-Multipathing-Plug-Ins oder das native Multipathing-Plug-In (NMP) handeln kann.

Allgemeine Informationen zu Multipathing-Plug-Ins finden Sie unter „Verwalten mehrerer Pfade“, auf Seite 22.

Für die durch das NMP-Modul verwalteten Pfade wird ein zweiter Satz von Beanspruchungsregeln angewendet. Diese Regeln legen fest, welches Speicher-Array-Typ-Plug-In (SATP) zum Verwalten der Pfade für einen bestimmten Array-Typ und welches Pfadauswahl-Plug-In (PSP) für die einzelnen Speichergeräte verwendet werden sollen. Beispielsweise ist für ein Speichergerät aus der EMC CLARiiON CX-Speicherfamilie, das nicht als ALUA-Gerät konfiguriert ist, das Standard-SATP „VMW_SATP_CX“ und das Standard-PSP „Zuletzt verwendet“.

Verwenden Sie den vSphere-Client, um anzuzeigen, welches SATP und PSP der Host für ein bestimmtes Speichergerät verwendet und welchen Status alle verfügbaren Pfade für dieses Speichergerät besitzen. Bei Bedarf können Sie das Standard-PSP von VMware mithilfe des vSphere-Clients ändern. Zum Ändern des Standard-SATPs müssen Sie die Beanspruchungsregeln unter Verwendung der vSphere-CLI ändern.

Informationen zum Ändern von Beanspruchungsregeln finden Sie unter „Verwalten von Speicherpfaden und Multipathing-Plug-Ins“, auf Seite 115.

Ausführliche Beschreibungen der Befehle für die PSA-Verwaltung finden Sie in den Handbüchern *vSphere Command-Line Interface Installation and Scripting Guide* und *vSphere Command-Line Interface Reference*.

Anzeigen der Pfadinformationen

Verwenden Sie den vSphere-Client, um anzuzeigen, welches SATP und PSP der ESX/ESXi-Host für ein bestimmtes Speichergerät verwendet und welchen Status alle verfügbaren Pfade für dieses Speichergerät besitzen. Sie können aus den Ansichten „Datenspeicher“ und „Geräte“ auf die Pfadinformationen zugreifen. Für Datenspeicher überprüfen Sie die Pfade, die eine Verbindung zu dem Gerät herstellen, auf dem der Datenspeicher bereitgestellt wird.

Zu den Pfadinformationen gehören das zum Verwalten des Geräts zugewiesene SATP, die Pfadauswahl-Richtlinie (PSP) und eine Liste von Pfaden mit ihren physischen Merkmalen, z. B. einem Adapter und einem Ziel, die von den einzelnen Pfaden verwendet werden, und dem Status der einzelnen Pfade. Es können die folgenden Informationen zum Pfadstatus angezeigt werden:

Aktiv — Pfade, die zum Senden von E/A an eine LUN verfügbar sind. Ein einzelner oder mehrere Arbeitspfade, die derzeit zur Übertragung von Daten verwendet werden, sind als „Aktiv (E/A)“ markiert.

HINWEIS Für Hosts, die ESX/ESXi 3.5 oder früher ausführen, bezeichnet der Begriff „Aktiv“ den einzigen Pfad, den der Host zum Senden von E/A an eine LUN verwendet.

Standby — Der Pfad ist verfügbar und kann für E/A verwendet werden, wenn aktive Pfade fehlschlagen.

Deaktiviert — Der Pfad wurde deaktiviert, sodass keine Daten übertragen werden können.

Ausgefallen — Die Software kann über diesen Pfad keine Verbindung mit der Festplatte herstellen.

Wenn Sie die Pfadrichtlinie **[Fest]** verwenden, können Sie erkennen, welcher Pfad der bevorzugte Pfad ist. Der bevorzugte Pfad ist mit einem Sternchen (*) in der bevorzugten Spalte gekennzeichnet.

Anzeigen von Datenspeicherpfaden

Verwenden Sie den vSphere-Client, um die Pfade zu überprüfen, die eine Verbindung zu Speichergeräten herstellen, auf denen die Datenspeicher bereitgestellt werden.

Vorgehensweise

1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenbereich auf den Server.

2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend unter **[Hardware]** auf **[Speicher (Storage)]** .

3 Klicken Sie unter „Ansicht“ auf **[Datenspeicher]** .

4 Wählen Sie in der Liste der konfigurierten Datenspeicher den Datenspeicher aus, dessen Pfade Sie anzeigen oder konfigurieren möchten.

   Im Fenster „Details“ wird die Gesamtanzahl an Pfaden angezeigt, die zum Zugriff auf das Gerät verwendet werden, sowie Informationen dazu, ob Pfade beschädigt oder deaktiviert sind.

5 Klicken Sie auf **[Eigenschaften] > [Pfade verwalten]** , um das Dialogfeld „Pfade verwalten“ zu öffnen.

   Sie können das Dialogfeld **[Pfade verwalten]** verwenden, um die Pfade zu aktivieren oder zu deaktivieren, die Multipathing-Richtlinie zu konfigurieren oder den bevorzugten Pfad anzugeben.

Anzeigen von Speichergerätepfaden

Verwenden Sie den vSphere-Client, um anzuzeigen, welches SATP und PSP der Host für ein bestimmtes Speichergerät verwendet und welchen Status alle verfügbaren Pfade für dieses Speichergerät besitzen.

Vorgehensweise

1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenbereich auf den Server.

2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend unter **[Hardware]** auf **[Speicher (Storage)]** .

3 Klicken Sie unter „Ansicht“ auf **[Geräte]** .

4 Klicken Sie auf **[Pfade verwalten (Manage Paths)]** , um das Dialogfeld **[Pfade verwalten (Manage Paths)]** zu öffnen.

Festlegen einer Pfadauswahl-Richtlinie

Der ESX/ESXi-Host legt für jedes Speichergerät die Pfadauswahl-Richtlinie auf Basis der in der Datei `/etc/vmware/esx.conf` definierten Beanspruchungsregeln fest.

Standardmäßig unterstützt VMware die folgenden Pfadauswahlrichtlinien: Wenn Sie die PSP eines Drittanbieters auf Ihrem Host installiert haben, wird die zugehörige Richtlinie ebenfalls in der Liste aufgeführt.

Feststehend (VMW_PSP_FIXED)
Der Host verwendet immer den bevorzugten Pfad zur Festplatte, wenn dieser Pfad verfügbar ist. Wenn nicht über den bevorzugten Pfad auf die Festplatte zugegriffen werden kann, versucht der Host, über die anderen Pfade auf die Festplatte zuzugreifen. Die Standardrichtlinie für Aktiv/Aktiv-Speichergeräte ist fest .

Fixed AP (VMW_PSP_FIXED_AP)
Erweitert die Funktionalität der Pfadrichtlinie „Feststehend“ auf Aktiv/Passiv- und ALUA-Modus-Arrays.

Zuletzt verwendet (VMW_PSP_MRU)
Der Host wählt den Pfad aus, den er kürzlich verwendet hat. Ist der Pfad nicht mehr verfügbar, wählt der Host einen alternativen Pfad aus. Der Host wird nicht auf den ursprünglichen Pfad zurückgesetzt, wenn dieser wieder verfügbar ist. Die MRU-Richtlinie beinhaltet keine Einstellung für den bevorzugten Pfad. MRU ist die Standardrichtlinie für Aktiv/Passiv-Speichergeräte.

Round Robin (VMW_PSP_RR)
Der Host verwendet einen automatischen Pfadauswahlalgorithmus, bei dem beim Verbinden mit Aktiv/Passiv-Arrays eine Rotation unter Berücksichtigung aller aktiven Pfade bzw. aller verfügbaren Pfade stattfindet. Dadurch wird ein Lastausgleich auf die für Ihren Host verfügbaren physischen Pfade implementiert.

Lastausgleich ist der Vorgang zum Verteilen der E/A-Anforderungen auf die Pfade. Das Ziel ist die Optimierung der Leistung im Hinblick auf den Durchsatz, z. B. E/A pro Sekunde, MB pro Sekunde oder Reaktionszeiten.

Tabelle 5-6 wird zusammengefasst, wie sich das Verhalten des Hosts abhängig vom Array-Typ und von der Failover-Richtlinie ändert.

Tabelle 5-6. Auswirkungen der Pfadrichtlinie

Richtlinie/Controller	Aktiv/Aktiv	Aktiv/Passiv
Zuletzt verwendet	Um nach einem Pfadausfall ein Failback durchzuführen, muss der Administrator einige Schritte ausführen.	Um nach einem Pfadausfall ein Failback durchzuführen, muss der Administrator einige Schritte ausführen.
Fest	Der VMkernel wird nach Wiederherstellung der Konnektivität unter Verwendung des bevorzugten Pfades fortgesetzt.	Es wird versucht, den VMkernel unter Verwendung des bevorzugten Pfades fortzusetzen. Dies kann zu Pfad-Thrashing oder einem Ausfall führen, wenn die LUN nun zu einem anderen Speicherprozessor gehört.
Round Robin	Kein Failback.	Der nächste Pfad in der Round-Robin-Planung wird ausgewählt.
Fixed AP	Für ALUA-Arrays wählt der VMkernel den als bevorzugten Pfad festgelegten Pfad. Für A/A- und A/P- sowie ALUA-Arrays wird der VMkernel unter Verwendung des bevorzugten Pfads fortgesetzt, jedoch nur, wenn der Algorithmus zur Vermeidung von Pfad-Thrashing das Failback zulässt.	

Ändern der Pfadauswahl-Richtlinie

In der Regel müssen Sie die standardmäßigen Multipathing-Einstellungen, die Ihr Host für ein bestimmtes Speichergerät verwendet, nicht ändern. Falls Sie jedoch Änderungen vornehmen möchten, können Sie im Dialogfeld „Pfade verwalten“ eine Pfadauswahl-Richtlinie ändern und den bevorzugten Pfad für die Richtlinie „Fest“ angeben.

Vorgehensweise

1 Öffnen Sie aus der Ansicht „Datenspeicher“ oder „Geräte“ das Dialogfeld „Pfade verwalten“.

2 Wählen Sie eine Pfadauswahlrichtlinie aus.

Standardmäßig unterstützt VMware die folgenden Pfadauswahlrichtlinien: Wenn Sie die PSP eines Drittanbieters auf Ihrem Host installiert haben, wird die zugehörige Richtlinie ebenfalls in der Liste aufgeführt.

- **[Feststehend (VMW_PSP_FIXED)]**
- **[Fixed AP (VMW_PSP_FIXED_AP)]**
- **[Zuletzt verwendet (VMW_PSP_MRU)]**
- **[Round Robin (VMW_PSP_RR)]**

3 Geben Sie für die Richtlinie „Fest“ den bevorzugten Pfad an, indem Sie mit der rechten Maustaste auf den Pfad klicken, den Sie als bevorzugten Pfad zuweisen möchten, und die Option **[Bevorzugt]** auswählen.

4 Klicken Sie auf **[OK]** , um Ihre Einstellungen zu speichern und das Dialogfeld zu schließen.

Deaktivieren von Pfaden

Pfade können zu Wartungszwecken oder aus anderen Gründen vorübergehend deaktiviert werden. Diese Aufgabe kann über den vSphere-Client ausgeführt werden.

Vorgehensweise

1 Öffnen Sie aus der Ansicht „Datenspeicher“ oder „Geräte“ das Dialogfeld „Pfade verwalten“.

2 Klicken Sie im Fenster „Pfade“ mit der rechten Maustaste auf den zu deaktivierenden Pfad und wählen Sie **[Deaktivieren]** .

3 Klicken Sie auf **[OK]** , um Ihre Einstellungen zu speichern und das Dialogfeld zu schließen.

Sie können einen Pfad auch aus der Ansicht „Pfade“ des Adapters deaktivieren, indem Sie in der Liste mit der rechten Maustaste auf den Pfad klicken und **[Deaktivieren]** wählen.

Pfadverwaltung und manueller oder statischer Lastausgleich

Durch den Lastausgleich für verfügbare Pfade wird die Leistung verbessert. Wenn Ihr Array das ALUA-Protokoll unterstützt, verwendet Ihr Host dieses Protokoll zur Durchführung des Lastausgleichs. Wenn Ihr Array das ALUA-Protokoll nicht unterstützt und Sie möchten, dass Ihr Host einen automatischen Lastausgleich durchführt, konfigurieren Sie Ihre Geräte für die Verwendung des Round Robin-PSPs. Wenn Sie den Lastausgleich selbst durchführen möchten, können Sie einen manuellen Lastausgleich durchführen.

Mit Aktiv-Aktiv- und Aktiv-Passiv-Speicher-Arrays können Sie Ihren Host zur Verwendung unterschiedlicher Pfade zu verschiedenen LUNs konfigurieren, um eine ausgeglichene Verwendung der Adapter zu erzielen. Wenn ein Pfad fehlschlägt, übernehmen die verbleibenden verfügbaren Pfade den gesamten Datenverkehr. Da das SAN möglicherweise mit einer neuen Topologie erstellt wird, um den Dienst wiederherzustellen, kann das Pfad-Failover eine Minute oder länger dauern. Diese Verzögerung ist erforderlich, damit nach einer Topologieänderung ein stabiler Zustand des SAN-Fabric hergestellt werden kann.

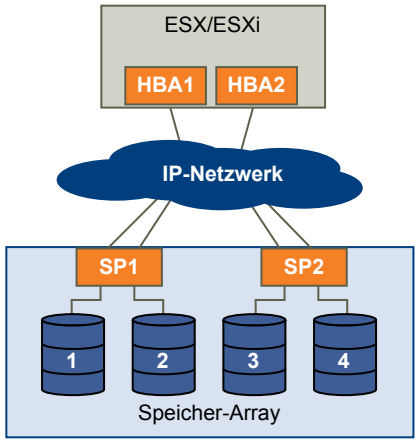
Sie können Ihren ESX/ESXi-Host so konfigurieren, dass der Datenverkehr auf mehrere Adapter verteilt wird, indem Sie Ihren LUNs bevorzugte Pfade zuweisen. Die Pfadrichtlinie muss auf „Fest“ gesetzt werden.

Das folgende Beispiel zeigt, wie der manuelle Lastausgleich mit einem Aktiv-Aktiv-Array durchgeführt wird.

Gehen wir von der folgenden Einrichtung aus, die in Abbildung 5-1 gezeigt ist.

- Aktiv/Aktiv-Speicherprozessoren
- Ein ESX/ESXi-System
- Zwei iSCSI-HBAs

Abbildung 5-1. Manueller Lastausgleich mit iSCSI



Für Lastausgleich legen Sie die bevorzugten Pfade wie folgt fest.

- Für LUN 1: HBA1-SP1-LUN1
- Für LUN 2: HBA2-SP1-LUN2
- Für LUN 3: HBA1-SP2-LUN3
- Für LUN 4: HBA2-SP2-LUN4

Mit Aktiv-Passiv-Arrays können Sie Lastausgleich durchführen, wenn das Array zwei aktive Pfade unterstützt und die HBA-Ports auf beide Speicherprozessoren in einem Array zugreifen können.

Sie können die Pfadauswahl-Richtlinie VMW_PSP_FIXED_AP verwenden, um einen Lastausgleich für statische Pfade auf Aktiv-Passiv-Arrays durchzuführen.

Festlegen der Zeitüberschreitung für das Gastbetriebssystem

Erhöhen Sie den standardmäßigen Zeitüberschreitungswert, um die Unterbrechung eines Windows-Gastbetriebssystems während des Failovers einzuschränken.

Das Pfad-Failover bezieht sich auf Situationen, in denen der aktive Pfad zu einer LUN in einen anderen Pfad geändert wird, üblicherweise weil eine SAN-Komponente ausgefallen ist, die den aktuellen Pfad verwendet.

E/A-Vorgänge können für 30 bis 60 Sekunden unterbrochen werden, bis der iSCSI-Treiber ermittelt, dass die Verbindung nicht mehr verfügbar ist, und ein Failover durchgeführt wird. Daher kann es den Anschein haben, als würden die virtuellen Maschinen (deren virtuelle Festplatten in einem SAN-Speicher installiert sind) nicht mehr reagieren. Beim Versuch, den Host, seine Speichergeräte oder seinen Adapter anzuzeigen, hat es möglicherweise den Anschein, als sei der Vorgang angehalten worden. Sobald das Failover abgeschlossen ist, werden die E/A-Vorgänge normal fortgesetzt.

Bei mehreren Unterbrechungen können sämtliche Verbindungen zu SAN-Speichergeräten verloren gehen. Wenn keine Verbindung zum Speichergerät funktioniert, treten für einige virtuelle Maschinen möglicherweise E/A-Fehler auf den virtuellen SCSI-Festplatten auf.

Für Windows 2000- und Windows Server 2003-Gastbetriebssysteme kann der Zeitüberschreitungswert über die Registrierung festgelegt werden.

Vorgehensweise

1 Sichern Sie die Windows-Registrierung.

2 Wählen Sie **[Start] > [Ausführen]** .

3 Geben Sie an der Befehlszeile **`regedit.exe`** ein und klicken Sie auf **[OK]** .

4 Doppelklicken Sie in der Hierarchiesicht auf der linken Seite auf **[HKEY_LOCAL_MACHINE]** , erweitern Sie **[System]** , **[CurrentControlSet]** und **[Services]** , und klicken Sie auf **[Disk]** .

5 Wählen Sie **[TimeOutValue]** , und setzen Sie den Datenwert auf x03c (hexadezimal) oder 60 (dezimal).

   Nach dem Durchführen dieser Änderung wartet Windows mindestens 60 Sekunden darauf, dass die verzögerten Festplattenoperationen abgeschlossen werden, bevor ein Fehler generiert wird.

6 Klicken Sie auf **[OK]** , um den **[Registrierungs-Editor]** zu schließen.

Gemeinsame Nutzung von Diagnosepartitionen

In der Regel verwenden Sie die lokale Festplatte Ihres ESX/ESXi-Hosts als Diagnosepartition. Bei ESX-Servern ohne Festplatten, die über ein SAN gestartet werden, können jedoch mehrere Hosts eine Diagnosepartition auf einer SAN-LUN gemeinsam verwenden.

Wenn mehrere ESX/ESXi-Systeme eine LUN als Diagnosepartition verwenden, muss für diese LUN eine Zone erstellt werden, sodass alle Server darauf zugreifen können.

Jeder Server benötigt 100 MB Speicherplatz, sodass die Größe der LUN die Anzahl an Servern bestimmt, die diese LUN gemeinsam verwenden. Jedes ESX/ESXi-System ist einem Diagnosesteckplatz zugeordnet. VMware empfiehlt mindestens 16 Steckplätze (1600 MB) Festplattenspeicher, wenn Server eine Diagnosepartition gemeinsam verwenden.

Wenn das Gerät lediglich über einen Diagnosesteckplatz verfügt, werden alle ESX/ESXi-Systeme, die dieses Gerät gemeinsam verwenden, demselben Steckplatz zugeordnet. Diese Einrichtung kann schnell zu Problemen führen. Wenn zwei ESX/ESXi-Systeme gleichzeitig einen Core-Dump erzeugen, werden die Core-Dumps auf der Diagnosepartition überschrieben.

Vermeiden und Beheben von SAN-Problemen

Bei Verwendung von ESX/ESXi in Verbindung mit einem SAN müssen Sie bestimmte Richtlinien befolgen, um SAN-Probleme zu vermeiden.

In diesem Abschnitt erhalten Sie einige Tipps, wie sich Probleme mit der SAN-Konfiguration vermeiden und beheben lassen:

- Platzieren Sie nur einen einzigen VMFS-Datenspeicher in jeder LUN. Mehrere VMFS-Datenspeicher in einer LUN werden nicht empfohlen.
- Ändern Sie die vom System festgelegte Pfadrichtlinie nur, wenn Sie die Auswirkungen dieser Änderung kennen und verstehen.
- Erstellen Sie eine ausführliche Dokumentation. Notieren Sie Informationen zu Konfiguration, Zugriffssteuerung, Speicher, Switch, Server und iSCSI-HBA-Konfiguration, Software- und Firmware-Versionen sowie zum Speicherkabelplan.
- Erstellen Sie einen Notfallplan bei Ausfällen:
  - Kopieren Sie Ihre Topologiezuordnungen mehrfach. Ermitteln Sie für jedes Element, welche Auswirkungen ein Ausfall dieses Elements auf das SAN hat.
  - Stellen Sie mithilfe einer Liste aller Verbindungen, Switches, HBAs und anderen Elemente sicher, dass Sie keine wichtige Fehlerstelle in Ihrem Design übersehen haben.
- Stellen Sie sicher, dass die iSCSI-HBAs an den geeigneten Steckplätzen des ESX/ESXi-Hosts installiert sind (basierend auf Steckplatz- und Busgeschwindigkeit). Richten Sie einen PCI-Bus-Lastausgleich für alle Busse des Servers ein.
- Machen Sie sich mit den verschiedenen Überwachungspunkten in Ihrem Speichernetzwerk an allen Sichtbarkeitspunkten vertraut (einschließlich ESX/ESXi-Leistungsdiagramme sowie Statistiken zu Ethernet-Switches und Speicherleistung)
- Seien Sie beim Ändern der IDs der LUNs vorsichtig, die über von Ihrem ESX/ESXi-Host verwendete VMFS-Datenspeicher verfügen. Wenn Sie die ID ändern, schlagen die auf dem VMFS-Datenspeicher ausgeführten virtuellen Maschinen fehl.

  Wenn sich keine laufenden virtuellen Maschinen auf dem VMFS-Datenspeicher befinden, nachdem Sie die ID der LUN geändert haben, müssen Sie zum Zurücksetzen der ID auf dem Host eine erneute Prüfung durchführen. Weitere Informationen über das erneute Prüfen finden Sie unter „Durchführen einer erneuten Speicherprüfung“, auf Seite 86.

Optimieren der SAN-Speicherleistung

Bei der Optimierung einer typischen SAN-Umgebung müssen verschiedene Faktoren berücksichtigt werden.

Bei ordnungsgemäßer Konfiguration der Netzwerkumgebung sollten die iSCSI-Komponenten einen ausreichenden Durchsatz und eine ausreichend geringe Latenz für iSCSI-Initiatoren und -Ziele bieten. Wenn das Netzwerk überlastet und die maximale Leistung von Verbindungen, Switches oder Routern erreicht ist, ist die iSCSI-Leistung beeinträchtigt und möglicherweise nicht mehr ausreichend für ESX/ESXi-Umgebungen.

Speichersystemleistung

Einer der wichtigsten Faktoren für die Optimierung einer kompletten iSCSI-Umgebung ist die Speichersystemleistung.

Bei Problemen mit der Speichersystemleistung lesen Sie die entsprechende Dokumentation des Speichersystem-Anbieters.

Bedenken Sie beim Zuweisen von LUNs, dass über verschiedene ESX/ESXi-Hosts auf jede gemeinsam genutzte LUN zugegriffen werden kann und dass auf jedem Host mehrere virtuelle Maschinen ausgeführt werden können. Auf einer LUN, die von einem ESX/ESXi-Host verwendet wird, sind E/A-Vorgänge von einer Vielzahl von unterschiedlichen Anwendungen möglich, die unter verschiedenen Betriebssystemen ausgeführt werden. Aufgrund dieser unterschiedlichen Arbeitslast sollte die RAID-Gruppe mit den ESX/ESXi-LUNs keine LUNs enthalten, die von anderen Hosts verwendet werden, auf denen nicht ESX/ESXi für E/A-intensive Anwendungen ausgeführt wird.

Aktivieren Sie die Lese- und Schreibcache.

Lastausgleich ist der Vorgang zum Verteilen von E/A-Anforderungen eines Servers auf alle verfügbaren Speicherprozessoren und die verknüpften Hostserverpfade. Das Ziel ist die Optimierung der Leistung im Hinblick auf den Durchsatz (E/A pro Sekunde, MB pro Sekunde oder Reaktionszeiten).

SAN-Speichersysteme müssen kontinuierlich neu ausgelegt und optimiert werden, um sicherzustellen, dass die E/A-Last auf alle Speichersystempfade verteilt ist. Um diese Anforderung zu erfüllen, verteilen Sie die Pfade zu den LUNs auf alle Speicherprozessoren. Das Ergebnis ist ein optimaler Lastausgleich. Eine sorgfältige Überwachung zeigt an, wenn die LUN-Verteilung manuell angepasst werden muss.

Bei der Optimierung von Speichersystemen mit statischem Lastausgleich ist die Überwachung der spezifischen Leistungsstatistiken (beispielsweise E/A-Vorgänge pro Sekunde, Blocks pro Sekunde und Reaktionszeit) und Verteilung der LUN-Arbeitslast auf alle Speicherprozessoren von größter Bedeutung.

HINWEIS Der dynamische Lastausgleich wird mit ESX/ESXi gegenwärtig nicht unterstützt.

Serverleistung

Um eine optimale Serverleistung sicherzustellen, müssen verschiedene Faktoren berücksichtigt werden.

Der Zugriff jeder Serveranwendung auf den integrierten Speicher muss mit den folgenden Bedingungen gewährleistet sein:

- Hohe E/A-Rate (Anzahl an E/A-Vorgängen pro Sekunde)
- Hoher Durchsatz (MB pro Sekunde)
- Minimale Latenz (Reaktionszeiten)

Da für jede Anwendung andere Anforderungen gelten, können Sie diese Ziele erreichen, indem Sie eine geeignete RAID-Gruppe für das Speichersystem wählen. Zum Erreichen von Leistungszielen führen Sie die folgenden Aufgaben aus:

- Platzieren Sie jede LUN in einer RAID-Gruppe, welche die erforderlichen Leistungsebenen bietet. Beachten Sie Aktivitäten und Ressourcennutzung von anderen LUNs in der zugewiesenen RAID-Gruppe. Mit einer hochleistungsfähigen RAID-Gruppe mit zu vielen Anwendungen, die eine E/A-Last verursachen, können die Leistungsziele möglicherweise nicht erreicht werden, die für eine Anwendung auf dem ESX/ESXi-Host erforderlich sind.
- Stellen Sie jeden Server mit einer ausreichenden Anzahl an iSCSI-Hardware-Adaptern bereit, um einen maximalen Durchsatz für alle Anwendungen zu ermöglichen, die während der Spitzenzeiten auf dem Server gehostet werden. Bei Verteilung der E/A-Last auf mehrere Ports wird ein höherer Durchsatz und eine geringere Latenz für jede Anwendung erreicht.

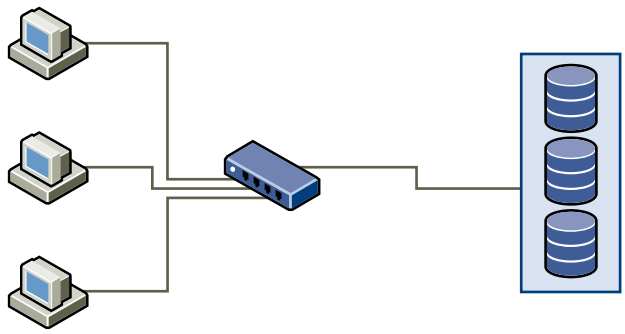
- Um für Software-iSCSI Redundanz zu bieten, verbinden Sie den Initiator mit allen Netzwerkadaptern, die für die iSCSI-Konnektivität verwendet werden.
- Beim Zuweisen von LUNs oder RAID-Gruppen für ESX/ESXi-Systeme werden diese Ressourcen durch mehrere Betriebssysteme gemeinsam verwendet. Daher kann die erforderliche Leistung jeder LUN im Speichersubsystem beim Einsatz von ESX/ESXi-Systemen deutlich höher sein als bei Verwendung von physischen Maschinen. Wenn Sie z. B. die Ausführung von vier E/A-intensiven Anwendungen planen, weisen Sie die vierfache Leistungskapazität für die ESX/ESXi-LUNs zu.
- Bei der gemeinsamen Verwendung mehrerer ESX/ESXi-Systeme mit vCenter Server, steigt die erforderliche Leistung für das Speichersubsystem entsprechend.
- Die Anzahl an ausstehenden E/A-Vorgängen von Anwendungen, die auf einem ESX/ESXi-System ausgeführt werden, sollte mit der Anzahl an E/A-Vorgängen übereinstimmen, die das SAN verarbeiten kann.

Netzwerkleistung

Ein typisches SAN umfasst verschiedene Computer, die über ein Netzwerk aus Switches mit verschiedenen Speichersystemen verbunden sind. Mehrere Computer greifen häufig auf denselben Speicher zu.

Abbildung 5-2 zeigt verschiedene Computersysteme, die über einen Ethernet-Switch mit einem Speichersystem verbunden sind. In dieser Konfiguration sind die einzelnen Systeme über eine einzige Ethernet-Verbindung mit dem Switch verbunden, der ebenfalls über eine einzige Ethernet-Verbindung mit dem Speichersystem verbunden ist. In den meisten Konfigurationen, mit modernen Switches und typischem Datenverkehr, stellt dies kein Problem dar.

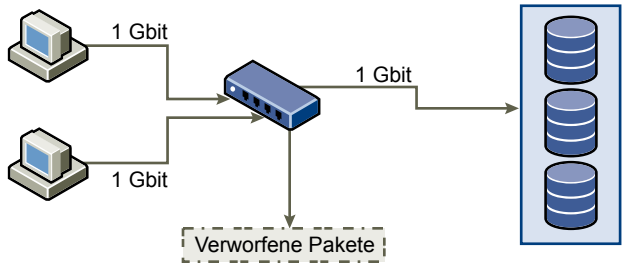
Abbildung 5-2. Eine einzige Ethernet-Verbindung mit dem Speicher



Wenn Systeme Daten aus dem Speicher lesen, ist die maximale Antwort des Speichers, genügend Daten zu senden, um die Verbindung zwischen den Speichersystemen und dem Ethernet-Switch zu füllen. Es ist unwahrscheinlich, dass ein einziges System oder eine einzige virtuelle Maschine die Netzwerkgeschwindigkeit vollständig nutzen kann. Wenn mehrere Systeme ein Speichergerät gemeinsam verwenden, ist dies jedoch die erwartete Situation.

Beim Schreiben von Daten in den Speicher versuchen möglicherweise mehrere Systeme oder virtuelle Maschinen, ihre Datenträger zu füllen. Wie Abbildung 5-3 zeigt, gehen in dieser Situation Daten zwischen den Systemen und dem Speichersystem verloren. Der Grund dafür ist, dass die zu übertragende Datenmenge die Kapazität einer einzigen Verbindung mit dem Speichersystem überschreitet. In diesem Fall verwirft der Switch Netzwerkpakete, da die Datenmenge, die übertragen werden kann, durch die Geschwindigkeit der Verbindung zwischen Switch und Speichersystem eingeschränkt ist.

Abbildung 5-3. Verworfene Pakete



Das Wiederherstellen von verworfenen Netzwerkpaketen führt zu einer erheblichen Leistungsbeeinträchtigung. Neben der Zeit zur Ermittlung, dass Daten verloren gegangen sind, ist für die erneute Übermittlung Netzwerkbandbreite erforderlich, die anderenfalls für aktuelle Transaktionen verwendet werden könnte.

iSCSI-Datenverkehr wird innerhalb des Netzwerks über TCP (Transmission Control Protocol) übermittelt. Bei TCP handelt es sich um ein zuverlässiges Übertragungsprotokoll, mit dem Sie sicherstellen, dass wiederholt versucht wird, verworfene Pakete zu übermitteln, bis diese ihr Ziel erreichen. TCP ist für eine Wiederherstellung und schnelle und problemlose Übermittlung von verworfenen Paketen konzipiert. Wenn der Switch jedoch regelmäßig Pakete verwirft, ist der Netzwerkdurchsatz deutlich reduziert. Das Netzwerk ist aufgrund von Anforderungen für ein erneutes Senden der Daten und durch die erneut gesendeten Pakete überlastet, und es werden letztendlich weniger Daten übertragen als in einem Netzwerk, das nicht überlastet ist.

Die meisten Ethernet-Switches können Daten puffern oder speichern, sodass jedes Gerät, das versucht Daten zu senden, die gleiche Möglichkeit hat, dieses Ziel zu erreichen. Diese Möglichkeit zum Puffern von Übertragungen erlaubt es, in Kombination mit einer Vielzahl an Systemen, die die Anzahl von ausstehenden Befehlen einschränken, kleine Datenpakete von mehreren Systemen der Reihe nach an ein Speichersystem zu senden.

Wenn bei umfangreichen Transaktionen mehrere Server versuchen, Daten über einen einzigen Switch-Port zu senden, kann die Kapazität des Switches zum Puffern einer Anforderung überschritten werden, während eine andere Anforderung übermittelt wird. In diesem Fall werden die Daten, die der Switch nicht senden kann, verworfen, und das Speichersystem muss die erneute Übermittlung des verworfenen Pakets anfordern. Wenn ein Ethernet-Switch an einem Eingangsport beispielsweise 32 KB puffern kann, der mit dem Switch verbundene Server jedoch annimmt, das 256 KB an das Speichergerät gesendet werden können, gehen einige Daten verloren.

Die meisten verwalteten Switches bieten Informationen zu verworfenen Paketen, die in etwa den folgenden Angaben entsprechen:

```
*: Schnittstelle ist verfügbar
IHQ: Gehaltene Pakete in Eingangswarteschlange     IQD: Verworfene Pakete in Eingangswarteschlan-
ge
OHQ: Gehaltene Pakete in Ausgangswarteschlange    OQD: Verworfene Pakete in Ausgangswarteschlange
RXBS: rx-Rate (Bit/s)          RXPS: rx-Rate (Pakete/s)
TXBS: tx-Rate (Bit/s)          TXPS: tx-Rate (Pakete/s)
TRTL: Drosselungswert
```

Tabelle 5-7. Beispiel zu Switch-Informationen

Schnitt-stelle	IHQ	IQD	OHQ	OQD	RXBS	RXPS	TXBS	TXPS	TRTL
*GigabitE-thernet0/1	3	9922	0	0	476303000	62273	477840000	63677	0

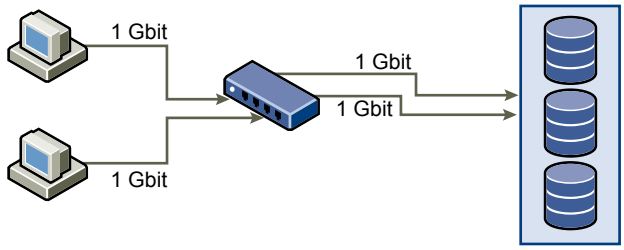
In diesem Beispiel eines Cisco-Switches lautet die verwendete Bandbreite 476303000 Bit/s, also weniger als die Hälfte der Kabelgeschwindigkeit. Trotzdem puffert die Schnittstelle eingehende Pakete, und es wurden einige Pakete verworfen. Die letzte Zeile dieser Schnittstellenübersicht zeigt, dass diese Schnittstelle bereits fast 10.000 eingehende Pakete in der IQD-Spalte verworfen hat.

Um dieses Problem zu verhindern, sind Konfigurationsänderungen erforderlich. Stellen Sie dabei sicher, dass eingehende Ethernet-Verbindungen nicht zu einer ausgehenden Verbindung zusammengefasst werden, sodass die Verbindung „überbucht“ wird. Wenn mehrere Verbindungen, deren Datenverkehr bereits fast die maximale Kapazität erreicht, zu einer kleineren Anzahl von Verbindungen zusammengefasst werden, ist eine Überbuchung möglich.

Im Allgemeinen sollten Anwendungen oder Systeme, die große Datenmengen in den Speicher schreiben (z. B. Datenerfassungs- oder Transaktionsprotokolliersysteme) keine gemeinsamen Ethernet-Verbindungen zu einem Speichergerät verwenden. Für diese Anwendungstypen wird mit mehreren Verbindungen zu Speichergeräten eine optimale Leistung erzielt.

Abbildung 5-4 zeigt mehrere Verbindungen vom Switch zum Speichergerät.

Abbildung 5-4. Mehrere Verbindungen zwischen Switch und Speicher



Die Verwendung von VLANs oder VPNs ist keine geeignete Lösung für das Problem von überlasteten Verbindungen in Konfigurationen mit gemeinsam verwendeten Komponenten. VLANs und andere Konfigurationen zur virtuellen Partitionierung von Netzwerken bieten eine Möglichkeit für den logischen Aufbau eines Netzwerks, ändern jedoch nicht die physischen Kapazitäten von Verbindungen und Trunks zwischen Switches. Wenn für den Speicherdatenverkehr und anderen Netzwerkverkehr gemeinsame physische Verbindungen verwendet werden (wie in einem VPN), besteht das Risiko von überlasteten Verbindungen und Paketverlust. Gleiches gilt für VLANs mit gemeinsamen Interswitch-Trunks. Für die Leistungsberechnungen in einem SAN müssen die physischen Grenzen des Netzwerks, nicht die logischen Zuordnungen berücksichtigt werden.

Beheben von Leistungsproblemen

Der vSphere-Client bietet umfangreiche Funktionen für das Erfassen von Leistungsdaten. Diese Informationen werden im vSphere-Client grafisch angezeigt. Die Anzeige des vSphere-Clients wird regelmäßig aktualisiert.

Sie können ebenfalls den vSphere-CLI-Befehl `resxtop` verwenden, um die Ressourcenverwendung auf ESX/ESXi-Hosts zu untersuchen. Weitere Informationen zu `resxtop` finden Sie im *Handbuch zur Ressourcenverwaltung* oder im Handbuch *vSphere Command-Line Interface Installation and Scripting Guide*.

Überprüfen von Ethernet-Switch-Statistiken

Eine Vielzahl von Ethernet-Switches bieten verschiedene Methoden zur Überwachung des Switch-Status.

Switches mit Ports, welche die meiste Zeit einen fast maximalen Durchsatz erzielen, bieten keine optimale Leistung. Wenn Sie in Ihrem iSCSI-SAN über solche Ports verfügen, reduzieren Sie die Last. Wenn der Port mit einem ESX/ESXi-System oder iSCSI-Speicher verbunden ist, kann die Last über einen manuellen Lastausgleich reduziert werden.

Wenn der Port mit mehreren Switches oder Routern verbunden ist, ziehen Sie die Installation zusätzlicher Verbindungen zwischen diesen Komponenten in Betracht, um eine höhere Last verarbeiten zu können. Ethernet-Switches bieten darüber hinaus meist Informationen zu Übertragungsfehlern, in der Warteschlange platzierten Paketen und verworfenen Ethernet-Paketen. Wenn ein Switch diese Bedingungen regelmäßig für Ports anzeigt, die für den iSCSI-Datenverkehr verwendet werden, bietet das iSCSI-SAN eine schlechte Leistung.

Problembehandlung bei Pfad-Thrashing

Wenn ein Server nicht auf eine LUN zugreifen kann, oder der Zugriff sehr langsam ist, liegt möglicherweise ein Problem mit Pfad-Thrashing (auch als LUN-Thrashing bezeichnet) vor. Ein Pfad-Thrashing kann auftreten, wenn zwei Hosts über unterschiedliche Speicherprozessoren auf die LUN zugreifen und die LUN zu keinem Zeitpunkt wirklich verfügbar ist.

Ein Pfad-Thrashing kann nur in spezifischen SAN-Konfigurationen mit den folgenden Bedingungen auftreten:

- Es wird ein Aktiv/Passiv-Array eingesetzt. Das Pfad-Thrashing tritt nur in Aktiv/Passiv-Arrays auf. Bei Aktiv/Aktiv-Arrays oder Arrays mit transparentem Failover, tritt kein Pfad-Thrashing auf.
- Zwei Hosts greifen gleichzeitig unter Verwendung verschiedener Speicherprozessoren auf dieselbe LUN zu. Dies kann auf zweierlei Weise passieren.
  - Die LUN ist beispielsweise zur Verwendung des festen PSPs konfiguriert. Auf Host A ist der bevorzugte Pfad zur LUN zur Verwendung eines Pfades über Speicherprozessor A angegeben. Auf Host B ist der bevorzugte Pfad zur LUN zur Verwendung eines Pfades über Speicherprozessor B angegeben.
  - Pfad-Thrashing kann auch stattfinden, wenn Host A auf die LUN nur mit Pfaden über SP A und Host B nur mit Pfaden über SP B zugreifen kann.

Dieses Problem kann ebenfalls bei direkt verbundenen Speicher-Arrays (z. B. AX100) mit HBA-Failover für einen oder mehrere Knoten auftreten.

Das Pfad-Thrashing ist ein Problem, das mit anderen Betriebssystemen üblicherweise nicht auftritt. Kein anderes Betriebssystem verwendet gemeinsame LUNs für mehr als zwei Server. Diese Konfiguration ist typischerweise für das Clustering reserviert.

Wenn jeweils nur ein Server E/A-Last generiert, stellt das Pfad-Trashing kein Problem dar. Mehrere ESX/ESXi-Systeme können jedoch gleichzeitig eine E/A-Last für dieselbe LUN erzeugen.

Grundlegendes zu Pfad-Thrashing

Die Speicherprozessoren in einem Speicher-Array sind mit unabhängigen Computern vergleichbar, die auf einen gemeinsamen Speicher zugreifen. Algorithmen bestimmen, wie der gleichzeitige Zugriff verarbeitet wird.

In Aktiv-Passiv-Arrays kann jeweils nur ein Speicherprozessor auf sämtliche Speicherbereiche zugreifen, die eine LUN umfasst. Der Besitz wird zwischen den Speicherprozessoren weitergegeben. Speichersysteme verwenden Zwischenspeicher, und Speicherprozessor A darf keine Daten auf die Festplatte schreiben, die den Zwischenspeicher von Speicherprozessor B ungültig machen. Da der Speicherprozessor den Zwischenspeicher nach dem Abschließen einer Operation leeren muss, kann der Besitz in kurzer Zeit verschoben werden. Während dieser Zeit kann keiner der beiden Speicherprozessoren E/A-Last für die LUN generieren.

Bei Aktiv-Aktiv-Arrays ermöglichen die Algorithmen einen präziseren Zugriff auf den Speicher sowie das Synchronisieren der Zwischenspeicher. Der Zugriff kann gleichzeitig durch mehrere Speicherprozessoren erfolgen, ohne dass ein zusätzlicher Zeitaufwand erforderlich ist.

Funktionsweise der Pfadauswahl:

- Bei einem Aktiv-Aktiv-Array beginnt das ESX/ESXi-System, E/A über den neuen Pfad zu senden.
- Bei Aktiv-Passiv-Arrays prüft das ESX/ESXi-System sämtliche Standby-Pfade. Der Speicherprozessor am Ende des gegenwärtig geprüften Pfades informiert das System darüber, ob er der aktuelle LUN-Besitzer ist.
  - Wenn das ESX/ESXi-System einen Speicherprozessor ermittelt, der die LUN besitzt, wird dieser Pfad ausgewählt und eine E/A-Anforderung über diesen Pfad gesendet.
  - Wenn der ESX/ESXi-Host keinen solchen Pfad ermitteln kann, wählt er einen der Pfade aus und sendet einen Befehl an den Speicherprozessor, damit dieser den LUN-Besitz an diesen Speicherprozessor übergibt.

  Das Pfad-Thrashing kann als Ergebnis der folgenden Pfadauswahl auftreten: Wenn Server A ausschließlich über einen Speicherprozessor auf eine LUN zugreifen kann, auf die auch Server B ausschließlich über einen anderen Speicherprozessor zugreifen kann, wechselt der LUN-Besitz kontinuierlich zwischen den beiden Speicherprozessoren. Da der Besitz schnell übergeben wird, kann das Speicher-Array keine E/A-Anforderung (oder nur eine nicht sehr umfangreiche) verarbeiten. Daher haben alle von einem LUN abhängigen Server aufgrund der langen Dauer für die Durchführung aller E/A-Anforderungen einen geringen Durchsatz.

Problembehandlung bei Pfad-Thrashing

Verwenden Sie das folgende Verfahren für die Problembehandlung bei Pfad-Thrashing. Ein Pfad-Thrashing kann auftreten, wenn zwei Hosts über unterschiedliche Speicherprozessoren auf die LUN zugreifen und die LUN zu keinem Zeitpunkt wirklich verfügbar ist.

Vorgehensweise

1. Stellen Sie sicher, dass alle Hosts, die eine Gruppe von LUNs in diesen Aktiv/Passiv-Arrays gemeinsam verwenden, gleichzeitig auf denselben Speicherprozessor zugreifen.
2. Korrigieren Sie mögliche Inkonsistenzen bei der Verkabelung oder der Maskierung unterschiedlicher ESX/ESXi-Hosts und SAN-Ziele, sodass allen HBAs dieselben Ziele in derselben Reihenfolge angezeigt werden.
3. Wählen Sie für die Pfadrichtlinie die Option „Zuletzt verwendet“ (Standardeinstellung) oder VMW_PSP_FIXED_AP.

Ausgleichen des Festplattenzugriffs zwischen virtuellen Maschinen

Die maximale Anzahl von ausstehenden Festplattenanforderungen kann im vSphere-Client über den Parameter `Disk.SchedNumReqOutstanding` festgelegt werden. Wenn zwei oder mehr virtuelle Maschinen auf dieselbe LUN zugreifen, steuert dieser Parameter die Anzahl an ausstehenden Anforderungen, die jede virtuelle Maschine an die LUN senden kann. Eine Anpassung der maximalen Anzahl kann sinnvoll sein, um den Festplattenzugriff zwischen virtuellen Maschinen auszugleichen.

Dieser Grenzwert findet keine Anwendung, wenn für eine LUN nur eine virtuelle Maschine aktiv ist. In diesem Fall ist die Bandbreite durch die Warteschlangentiefe des Speicheradapters eingeschränkt.

Vorgehensweise

1. Wählen Sie im Bestandslistenbereich des vSphere-Clients den gewünschten Host aus.
2. Klicken Sie auf die Registerkarte **[Konfiguration]** und dann unter „Software“ auf **[Erweiterte Einstellungen (Advanced Settings)]** .

3 Klicken Sie im linken Fenster auf **[Festplatte]** , und führen Sie einen Bildlauf zu **[Disk.SchedNumReqOutstanding]** durch.

4 Ändern Sie den Parameterwert auf die gewünschte Zahl ab, und klicken Sie auf **[OK]** .

Diese Änderung kann die Planung der Festplattenbandbreite beeinflussen, bei festplattenintensiven Arbeitslasten jedoch zu Verbesserungen führen.

Weiter

Wenn Sie diesen Wert im VMkernel ändern, sollten Sie möglicherweise auch die Warteschlangentiefe des Speicheradapters anpassen.

Festlegen der maximalen Warteschlangentiefe für Software-iSCSI

Wenn für Software-iSCSI-LUNs eine nicht zufriedenstellende Leistung erzielt wird, kann die maximale Warteschlangentiefe über den Befehl `vicfg-module` geändert werden.

Vorgehensweise

1 Führen Sie an der vSphere-CLI den folgenden Befehl aus:

```
vicfg-module -s iscsivmk_LunQDepth=Wert iscsi_vmk
```

Der Parameter `iscsivmk_LunQDepth` legt die maximale Anzahl ausstehender Befehle oder die Warteschlangentiefe für jede LUN fest, auf die über den Software-iSCSI-Adapter zugegriffen wird. Der Standardwert ist 128.

2 Starten Sie Ihr System neu.

Vorsicht Wenn für die Warteschlangentiefe ein höherer Wert als die Standardeinstellung gewählt wird, kann die Gesamtzahl an unterstützten LUNs reduziert sein.

Reduzieren von SCSI-Reservierungen

Vorgänge, für die eine Dateisperre oder Metadatensperre in VMFS erforderlich ist, führen zu kurzzeitigen SCSI-Reservierungen. SCSI-Reservierungen sperren eine LUN vollständig. Eine übermäßig hohe Anzahl an SCSI-Reservierungen durch einen Server kann die Leistung auf anderen Servern beeinträchtigen, die auf dasselbe VMFS zugreifen.

Im Folgenden sind Beispiele für Vorgänge aufgelistet, die Datei- oder Metadatensperren erfordern:

- Einschaltvorgänge für virtuelle Maschinen
- VMotion.
- Virtuelle Maschinen, die mit Snapshots virtueller Festplatten ausgeführt werden
- Dateivorgänge, die das Öffnen von Dateien oder Updates von Metadaten erfordern.

Hinweis ESX/ESXi verwendet den SCSI-Reservierungsmechanismus nur dann, wenn eine LUN nicht VAAI-fähig ist. Wenn eine LUN VAAI-fähig ist und die Hardwarebeschleunigung unterstützt, verwendet ESX/ESXi den ATS-Algorithmus (ATS, Atomic Test and Set), um die LUN zu sperren.

Wenn diese Vorgänge häufig auf mehreren Servern durchgeführt werden, die auf dasselbe VMFS zugreifen, kann die Leistung beeinträchtigt sein. VMware rät beispielsweise davon ab, eine Vielzahl von virtuellen Maschinen auf mehreren Servern auszuführen, die Snapshots virtueller Festplatten in demselben VMFS verwenden. Beschränken Sie die Anzahl an VMFS-Dateivorgängen, wenn eine Vielzahl von virtuellen Maschinen in dem VMFS ausgeführt werden.

Überlegungen zu SAN-Speichersicherungen

In der SAN-Umgebung haben Sicherungen zwei Ziele. Das erste Ziel ist die Archivierung von Onlinedaten als Offlinemedien. Dieser Vorgang wird gemäß eines festgelegten Zeitplans regelmäßig für alle Onlinedaten wiederholt. Das zweite Ziel ist der Zugriff auf Offlinedaten zu Wiederherstellungszwecken. Für die Datenbankwiederherstellung müssen z. B. häufig archivierte Protokolldateien abgerufen werden, die gegenwärtig nicht online sind.

Die Planung von Sicherungen hängt von verschiedenen Faktoren ab:

- Ermittlung von kritischen Anwendungen, die häufigere Sicherungszyklen innerhalb eines bestimmten Zeitraums erfordern.
- Ziele für Wiederherstellungspunkte und -zeiten. Überlegen Sie, wie präzise Ihr Wiederherstellungspunkt sein muss und wie lange Sie darauf warten können.
- Die mit den Daten verknüpfte Änderungsrate (Rate of Change, RoC). Wenn Sie beispielsweise die synchrone bzw. asynchrone Replikation verwenden, beeinflusst die RoC die erforderliche Bandbreite zwischen den primären und den sekundären Speichergeräten.
- Auswirkungen insgesamt auf die SAN-Umgebung, Speicherleistung (während der Sicherung) und andere Anwendungen.
- Ermittlung von Spitzenzeiten für den Datenverkehr im SAN (Sicherungen, die während dieser Spitzenzeiten geplant werden, können die Anwendungen und den Sicherungsprozess verlangsamen).
- Zeit für das Planen aller Sicherungen im Datencenter.
- Zeit für das Sichern einer einzelnen Anwendung.
- Ressourcenverfügbarkeit für die Datenarchivierung; üblicherweise Zugriff auf Offlinedaten (Band).

Planen Sie für jede Anwendung ein Wiederherstellungszeitziel (Recovery Time Objective, RTO), wenn Sie die Sicherungsstrategie entwerfen. Das heißt, berücksichtigen Sie die Zeit und Ressourcen, die zur erneuten Bereitstellung der Daten erforderlich sind. Wenn eine geplante Sicherung beispielsweise eine so große Datenmenge speichert, dass die Wiederherstellung sehr lange dauert, überprüfen Sie die geplante Sicherung. Führen Sie die Sicherung häufiger durch, um die gespeicherte Datenmenge pro Sicherungsvorgang und die Wiederherstellungszeit zu reduzieren.

Wenn eine Anwendung innerhalb eines bestimmten Zeitraums wiederhergestellt werden muss, muss der Sicherungsvorgang einen Zeitplan und eine spezielle Datenverarbeitung bieten, um diese Anforderung zu erfüllen. Eine schnelle Wiederherstellung kann die Verwendung von Wiederherstellungs-Volumes in einem Onlinespeicher erfordern, um die Notwendigkeit des Zugriffs auf langsame Offlinemedien für fehlende Datenkomponenten zu minimieren oder zu eliminieren.

Snapshot-Software

Mithilfe von Snapshot-Software können Administratoren umgehend eine Kopie einer einzelnen virtuellen Festplatte erstellen, die im Festplattensubsystem definiert ist.

Snapshot-Software ist für unterschiedliche Ebenen verfügbar:

- ESX/ESXi-Hosts ermöglichen die Snapshot-Erstellung für virtuelle Maschinen. Diese Software ist im ESX/ESXi-Basispaket enthalten.
- Sicherungssoftware anderer Anbieter kann umfangreichere Sicherungen bieten und erweiterte Konfigurationsoptionen umfassen.

Administratoren erstellen Snapshots u. a. zu folgenden Zwecken:

- Sicherung
- Notfallwiederherstellung

- Verfügbarkeit mehrerer Konfigurationen oder Versionen bzw. beides
- Diagnose (Untersuchen von Snapshots zur Ermittlung einer Fehlerursache, während das System ausgeführt wird)
- Data-Mining (Untersuchen einer Datenkopie, um die Last in Produktionssystemen zu reduzieren)

Verwenden von Drittanbieter-Sicherungspaketen

Die Verwendung von Drittanbietersoftware bietet den Vorteil einer einheitlichen Umgebung. Die zusätzlichen Kosten für die Snapshot-Software anderer Anbieter können bei Erweiterung Ihres SAN jedoch steigen.

Stellen Sie bei Verwendung von Drittanbieter-Sicherungssoftware sicher, dass die Software mit ESX/ESXi-Hosts unterstützt wird.

Beachten Sie bei Verwendung von Snapshots zum Sichern Ihrer Daten die folgenden Punkte:

- Einige Anbieter unterstützen Snapshots sowohl für VMFS als auch für RDMs. Werden beide unterstützt, können Sie entweder einen Snapshot des gesamten Dateisystems der virtuellen Maschine für einen Host oder Snapshots einzelner virtueller Maschinen (eine pro Festplatte) erstellen.
- Einige Anbieter unterstützen Snapshots nur für Einrichtungen mit RDMs. Werden nur RDMs unterstützt, können Sie Snapshots einzelner virtueller Maschinen erstellen.

Weitere Informationen finden Sie in der Dokumentation Ihres Speicheranbieters.

HINWEIS ESX/ESXi-Systeme umfassen ebenfalls eine Consolidated Backup-Komponente.

Mehrschichtige Anwendungen

SAN-Administratoren verwenden üblicherweise spezialisierte Array-basierte Software für Sicherung, Notfallwiederherstellung, Data-Mining, Diagnose und Konfigurationstests.

Speicheranbieter stellen typischerweise zwei Arten von erweiterten Diensten für ihre LUNs bereit: Snapshot-Erstellung und Replikation.

Wenn Sie ein ESX/ESXi-System in Verbindung mit einem SAN verwenden, ermitteln Sie, ob sich Array-basierte oder hostbasierte Tools für Ihre individuelle Situation besser eignen.

Array-basierte Lösung (Drittanbieter)

Wenn Sie ein ESX/ESXi-System in Verbindung mit einem SAN verwenden, ermitteln Sie, ob sich Array-basierte für Ihre individuelle Situation besser eignen.

Wenn Sie eine Array-basierte Lösung in Betracht ziehen, berücksichtigen Sie Folgendes:

- Array-basierte Lösungen bieten meist umfangreichere Statistiken. Da Daten bei RDM immer über denselben Pfad übermittelt werden, ist die Leistungsverwaltung vereinfacht.
- Die Sicherheit ist für den Speicheradministrator bei Verwendung von RDM und einer Array-basierten Lösung transparenter, da virtuelle Maschinen mit RDM eher mit physischen Maschinen vergleichbar sind.
- Bei Einsatz einer Array-basierten Lösung werden RDMs im physischen Kompatibilitätsmodus häufig zum Speichern von virtuellen Maschinen verwendet. Wenn kein RDM verwendet werden soll, erfahren Sie in der Dokumentation des Speicheranbieters, ob Vorgänge auf LUNs mit VMFS-Volumes unterstützt werden. Lesen Sie bei Verwendung von Array-Vorgängen auf VMFS-LUNs ferner den Abschnitt zur Neusignierung sorgfältig.

Dateibasierte Lösung (VMFS)

Wenn Sie ein ESX/ESX-System in Verbindung mit einem SAN verwenden, ermitteln Sie, ob sich hostbasierte Tools für Ihre individuelle Situation besser eignen.

Wenn Sie den Einsatz einer dateibasierten Lösung erwägen, welche die VMware Tools und VMFS anstelle der Array-Tools verwendet, beachten Sie die folgenden Punkte:

- Die Verwendung der VMware Tools mit VMFS bietet eine bessere Bereitstellung. Es wird eine große LUN zugeteilt, und mehrere `.vmdk`-Dateien können in dieser LUN platziert werden. Bei RDM ist für jede virtuelle Maschine eine neue LUN erforderlich.
- Eine Funktion zur Snapshot-Erstellung ist auf Ihrem ESX/ESXi-Host ohne zusätzliche Kosten enthalten. Aus diesem Grund ist die dateibasierte Lösung kosteneffektiver als die Array-basierte Lösung.
- Die Verwendung von VMFS ist einfacher für ESX/ESXi-Administratoren.
- ESX/ESXi-Administratoren, die eine dateibasierte Lösung einsetzen, sind vom SAN-Administrator unabhängiger.

Verwalten von duplizierten VMFS-Datenspeichern

Wenn eine LUN eine Kopie eines VMFS-Datenspeichers enthält, können Sie den Datenspeicher mit der vorhandenen Signatur mounten oder eine neue Signatur zuweisen.

Jeder in einer LUN erstellte VMFS-Datenspeicher besitzt eine eindeutige UUID, die im Superblock des Dateisystems gespeichert ist. Wenn die LUN repliziert oder ein Snapshot von ihr erstellt wird, ist die dabei entstehende LUN-Kopie Byte für Byte mit der ursprünglichen LUN identisch. Wenn die ursprüngliche LUN einen VMFS-Datenspeicher mit der UUID X enthält, scheint daher die LUN-Kopie einen identischen VMFS-Datenspeicher bzw. eine VMFS-Datenspeicherkopie mit genau derselben UUID X zu enthalten.

ESX/ESXi kann ermitteln, ob eine LUN die VMFS-Datenspeicherkopie enthält, und entweder die Datenspeicherkopie mit ihrer ursprünglichen UUID mounten oder die UUID ändern, wodurch der Datenspeicher neu signiert wird.

Mounten von VMFS-Datenspeichern mit vorhandenen Signaturen

In bestimmten Fällen ist das Neusignieren einer VMFS-Datenspeicherkopie möglicherweise nicht erforderlich. Sie können eine VMFS-Datenspeicherkopie mounten, ohne ihre Signatur zu ändern.

Sie können beispielsweise synchronisierte Kopien von virtuellen Maschinen als Teil eines Notfallplans auf einer sekundären Site unterhalten und bei einem Notfall an der primären Site die Datenspeicherkopie auf den virtuellen Maschinen der sekundären Site einschalten.

Wichtig Sie können eine VMFS-Datenspeicherkopie nur mounten, wenn sie nicht mit dem ursprünglichen VMFS-Datenspeicher, der über dieselbe UUID verfügt, kollidiert. Zum Mounten der Kopie muss der ursprüngliche VMFS-Datenspeicher offline sein.

Wenn Sie den VMFS-Datenspeicher mounten, lässt ESX/ESXi Lese- und Schreibvorgänge in den Datenspeicher zu, der sich auf der LUN-Kopie befindet. Die LUN-Kopie darf nicht schreibgeschützt sein. Die Datenspeicher-Mounts sind über Systemneustarts hinweg dauerhaft und gültig.

Da ESX/ESXi das Neusignieren des gemounteten Datenspeichers nicht zulässt, müssen Sie den Datenspeicher vor dem Neusignieren unmounten.

Mounten eines VMFS-Datenspeichers mit einer vorhandenen Signatur

Wenn Sie eine Kopie eines VMFS-Datenspeichers nicht neu signieren müssen, können Sie sie mounten, ohne ihre Signatur zu ändern.

Voraussetzungen

Führen Sie vor dem Mounten eines VMFS-Datenspeichers eine erneute Speicherprüfung auf Ihrem Host durch, sodass er seine Ansicht der ihm präsentierten LUNs aktualisiert.

Vorgehensweise

1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenbereich auf den Server.

2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend unter **[Hardware]** auf **[Speicher (Storage)]** .

3 Klicken Sie auf **[Speicher hinzufügen]** .

4 Markieren Sie den Speichertyp **[Festplatte/LUN (Disk/LUN)]** , und klicken Sie auf **[Weiter]** .

5 Wählen Sie in der Liste der LUNs die LUN aus, die einen Datenspeichernamen in der Spalte „VMFS-Bezeichnung“ enthält, und klicken Sie auf **[Weiter]** .

   Der in der Spalte „VMFS-Bezeichnung“ vorhandene Name gibt an, dass die LUN eine Kopie ist, die eine Kopie eines vorhandenen VMFS-Datenspeichers enthält.

6 Wählen Sie unter „Optionen für das Mounten“ die Option **[Vorhandene Signatur beibehalten]** aus.

7 Überprüfen Sie auf der Seite **[Bereit zum Abschließen (Ready to Complete)]** die Informationen zur Datenspeicherkonfiguration, und klicken Sie auf **[Beenden]** .

Weiter

Wenn Sie den gemounteten Datenspeicher zu einem späteren Zeitpunkt erneut signieren möchten, müssen Sie ihn zunächst unmounten.

Unmounten von Datenspeichern

Wenn Sie einen Datenspeicher unmounten, bleibt dieser intakt, er wird jedoch von den von Ihnen angegebenen Hosts nicht mehr angezeigt. Er wird weiterhin auf anderen Hosts angezeigt, auf denen er gemountet bleibt.

Sie können nur die folgenden Typen von Datenspeichern unmounten:

- NFS-Datenspeicher
- VMFS-Datenspeicherkopien, die ohne Neusignierung gemountet wurden

Sie können einen aktiven gemounteten Datenspeicher nicht unmounten.

Vorgehensweise

1 Zeigen Sie die Datenspeicher an.

2 Klicken Sie mit der rechten Maustaste auf den entsprechenden Datenspeicher und wählen Sie **[Unmounten]** .

3 Wenn der Datenspeicher gemeinsam genutzt wird, geben Sie an, welche Hosts nicht mehr auf den Datenspeicher zugreifen sollen.

   a Heben Sie ggf. die Auswahl der Hosts auf, auf denen der Datenspeicher gemountet bleiben soll.

   Standardmäßig sind alle Hosts ausgewählt.

   b Klicken Sie auf **[Weiter]** .

   c Überprüfen Sie die Liste der Hosts, von denen Sie den Datenspeicher unmounten möchten, und klicken Sie auf **[Beenden]** .

4 Bestätigen Sie, dass Sie den Datenspeicher unmounten möchten.

Neusignieren von VMFS-Kopien

Verwenden Sie die Datenspeicher-Neusignierung, wenn Sie die in der Kopie des VMFS-Datenspeichers gespeicherten Daten aufbewahren möchten. Beim Neusignieren einer VMFS-Kopie weist ESX/ESXi der Kopie eine neue UUID und eine neue Bezeichnung zu und mountet die Kopie als einen vom Original unabhängigen Datenspeicher.

Die neue Bezeichnung, die dem Datenspeicher zugewiesen wird, besitzt das Standardformat `snap-`*`Snap-ID`*`-`*`Alte_Bezeichnung`*, wobei*Snap-ID* für eine Ganzzahl und *Alte_Bezeichnung* für die Bezeichnung des ursprünglichen Datenspeichers steht.

Beachten Sie bei der Datenspeicher-Neusignierung Folgendes:

- Die Datenspeicher-Neusignierung kann nicht rückgängig gemacht werden.
- Die LUN-Kopie, die den VMFS-Datenspeicher enthält, der neu signiert wird, wird nicht länger als LUN-Kopie behandelt.
- Ein übergreifender Datenspeicher kann nur neu signiert werden, wenn all seine Erweiterungen online sind.
- Der Neusignierungsprozess ist absturz- und fehlertolerant. Wenn der Prozess unterbrochen wird, können Sie ihn später fortsetzen.
- Sie können den neuen VMFS-Datenspeicher mounten, ohne dass das Risiko besteht, dass seine UUID mit UUIDs anderer Datenspeicher, wie z. B. einem über- oder untergeordneten Datenspeicher in einer Hierarchie von LUN-Snapshots, kollidiert.

Neusignieren einer VMFS-Datenspeicherkopie

Verwenden Sie die Datenspeicher-Neusignierung, wenn Sie die in der Kopie des VMFS-Datenspeichers gespeicherten Daten aufbewahren möchten.

Voraussetzungen

Wenn Sie eine gemountete Datenspeicherkopie neu signieren möchten, müssen Sie sie zunächst unmounten.

Führen Sie vor dem Neusignieren eines VMFS-Datenspeichers eine erneute Speicherprüfung auf Ihrem Host durch, sodass der Host seine Ansicht der ihm präsentierten LUNs aktualisiert und vorhandene LUN-Kopien erkennt.

Vorgehensweise

1 Melden Sie sich am vSphere-Client an, und klicken Sie im Bestandslistenbereich auf den Server.

2 Klicken Sie auf die Registerkarte **[Konfiguration]** und anschließend unter **[Hardware]** auf **[Speicher (Storage)]** .

3 Klicken Sie auf **[Speicher hinzufügen]** .

4 Markieren Sie den Speichertyp **[Festplatte/LUN (Disk/LUN)]** , und klicken Sie auf **[Weiter]** .

5 Wählen Sie in der Liste der LUNs die LUN aus, die einen Datenspeichernamen in der Spalte „VMFS-Bezeichnung“ enthält, und klicken Sie auf **[Weiter]** .

Der in der Spalte „VMFS-Bezeichnung“ vorhandene Name gibt an, dass die LUN eine Kopie ist, die eine Kopie eines vorhandenen VMFS-Datenspeichers enthält.

6 Wählen Sie unter „Optionen für das Mounten“ die Option **[Neue Signatur zuweisen]** aus und klicken Sie auf **[Weiter]** .

7 Überprüfen Sie auf der Seite **[Bereit zum Abschließen (Ready to Complete)]** die Informationen zur Datenspeicherkonfiguration, und klicken Sie auf **[Beenden]** .

Weiter

Nach der erneuten Signierung sind möglicherweise die folgenden Schritte erforderlich:

- Wenn die neu signierten Datenspeicher virtuelle Maschinen enthalten, aktualisieren Sie die Referenzen auf den VMFS-Datenspeicher in den Dateien der virtuellen Maschine, darunter die Dateien mit den Erweiterungen `.vmx`, `.vmdk`, `.vmsd` und `.vmsn`.
- Registrieren Sie virtuelle Maschinen mit vCenter Server, wenn Sie sie einschalten möchten.

Speicherhardware-Beschleunigung

Die Hardwarebeschleunigungs-Funktion ermöglicht Ihrem Host die Auslagerung bestimmter VM- und Speicherverwaltungsvorgänge in konforme Speicherhardware. Mit der Speicherhardware-Unterstützung führt Ihr Host diese Vorgänge schneller aus und verbraucht weniger CPU, Arbeitsspeicher und Speicher-Fabric-Bandbreite.

Zur Implementierung der Hardwarebeschleunigungs-Funktion verwendet die PSA (Pluggable Storage Architecture) eine Kombination aus speziellen Array-Integrations-Plug-Ins (als VAAI-Plug-Ins bezeichnet) und einem Array-Integrationsfilter (als VAAI-Filter bezeichnet). Die PSA hängt den VAAI-Filter und anbieterspezifische VAAI-Plug-Ins automatisch an die Speichergeräte an, die die Hardwarebeschleunigung unterstützen.

Verwenden Sie zum Anzeigen und Verwalten des VAAI-Filters und der VAAI-Plug-Ins, die auf Ihrem Host verfügbar sind, die vSphere-CLI-Befehle.

Informationen zum Verwalten des VAAI-Filters und der VAAI-Plug-Ins finden Sie unter „Verwalten des Hardwarebeschleunigungsfilters und der Hardwarebeschleunigungs-Plug-Ins“, auf Seite 122.

Beschreibungen der Befehle finden Sie in den Handbüchern *vSphere Command-Line Interface Installation and Scripting Guide* und *vSphere Command-Line Interface Reference*.

Anforderungen und Vorteile der Hardwarebeschleunigung

Die Hardwarebeschleunigungs-Funktion kann nur mit einer geeigneten Kombination aus Host und Speicher-Array verwendet werden.

Verwenden Sie die folgenden Hosts und Speicher-Arrays:

- ESX/ESXi Version 4.1 oder höher.
- Speicher-Arrays, die die speicherbasierte Hardwarebeschleunigung unterstützen. ESX/ESXi Version 4.1 bietet keine Unterstützung für die Hardwarebeschleunigung mit NAS-Speichergeräten.

Auf Ihrem Host ist die Hardwarebeschleunigung standardmäßig aktiviert. Wenn Sie die Hardwarebeschleunigung auf der Speicherseite aktivieren möchten, wenden Sie sich an den Speicheranbieter. Bestimmte Speicher-Arrays erfordern, dass Sie die Hardwarebeschleunigungs-Unterstützung auf der Speicherseite explizit aktivieren.

Wenn die Hardwarebeschleunigungs-Funktion unterstützt wird, kann der Host Hardwareunterstützung erhalten und die folgenden Vorgänge schneller und effizienter ausführen:

- Die Migration virtueller Maschinen mit Storage VMotion
- Die Bereitstellung virtueller Maschinen anhand von Vorlagen
- Das Klonen virtueller Maschinen oder Vorlagen
- VMFS Clustered Locking und Metadatenvorgänge für Dateien virtueller Maschinen
- Schreibvorgänge auf virtuelle Festplatten der Formate „Schnell bereitgestellt“ und „Thick“
- Erstellung fehlertoleranter virtueller Maschinen

Status der Hardwarebeschleunigungs-Unterstützung

Für jedes Speichergerät und jeden Datenspeicher zeigt der vSphere-Client den Status der Hardwarebeschleunigungs-Unterstützung in der Spalte „Hardwarebeschleunigung“ der Ansichten „Geräte“ und „Datenspeicher“ an.

Die Statuswerte lauten „Unbekannt“, „Unterstützt“ und „Nicht unterstützt“. Der Anfangswert ist „Unbekannt“. Der Status ändert sich in „Unterstützt“, wenn der Host den Auslagerungsvorgang erfolgreich ausgeführt hat. Wenn der Auslagerungsvorgang fehlschlägt, ändert sich der Status in „Nicht unterstützt“.

Wenn Speichergeräte die Hostvorgänge nicht oder nur teilweise unterstützen, kehrt der Host für die Ausführung nicht unterstützter Vorgänge zu seinen nativen Methoden zurück.

Ausschalten der Hardwarebeschleunigung

Falls Ihre Speichergeräte die Hardwarebeschleunigungs-Funktion nicht unterstützen, können Sie sie mithilfe der erweiterten Einstellungen des vSphere-Clients deaktivieren.

Wenden Sie sich, wie bei allen erweiterten Einstellungen, an den VMware-Support, bevor Sie die Hardwarebeschleunigung deaktivieren.

Vorgehensweise

1 Wählen Sie im Bestandslistenbereich des vSphere-Clients den Host aus.

2 Klicken Sie auf die Registerkarte **[Konfiguration]** und dann unter **[Software]** auf **[Erweiterte Einstellungen]** .

3 Klicken Sie auf „VMFS3“ und ändern Sie den Wert im Feld **[VMFS3.HardwareAcceleratedLocking]** in Null.

4 Klicken Sie auf **[DataMover]** und ändern Sie die Werte in allen folgenden Feldern in Null:

- **[DataMover.HardwareAcceleratedMove]**
- **[DataMover.HardwareAcceleratedInit]**

5 Klicken Sie auf **[OK]** , um Ihre Änderungen zu speichern.

iSCSI SAN-Konfiguration - Checkliste A

Dieses Thema bietet eine Checkliste mit speziellen Installationsanforderungen für verschiedene Speichersysteme und ESX/ESXi-Hosts.

Tabelle A-1. iSCSI SAN-Konfigurationsanforderungen

Komponente	Anmerkungen
Alle Speichersysteme	Schreibcache muss deaktiviert sein, falls dieser nicht durch einen Akku gesichert ist.
Topologie	Ein HBA- oder SP-Failover sollte nicht durch eine Einzelfehlerstelle verursacht werden, speziell bei Speicher-Arrays vom Typ „Aktiv/Passiv“.
EMC Symmetrix	Aktivieren Sie die SPC2- und SC3-Einstellungen. Aktuelle Einstellungen erhalten Sie von EMC.
EMC Clariion	Legen Sie den EMC Clariion-Failover-Modus auf 1 oder 4 fest. Wenden Sie sich an EMC für weitere Einzelheiten.
HP MSA	Keine spezifischen Anforderungen
HP EVA	Setzen Sie den Hosttyp für EVA3000/5000 mit Firmware der Version 4.001 oder höher und EVA4000/6000/8000 mit Firmware der Version 5.031 und höher auf `VMware`. In allen anderen Fällen setzen Sie den Hostmodustyp auf `Benutzerdefiniert`. Der Wert lautet: ■ EVA3000/5000 mit Firmware der Version 3.x: 000000002200282E ■ EVA4000/6000/8000: 000000202200083E
NetApp	Wenn einer Ihrer iSCSI-Initiatoren Teil einer Initiatorgruppe (igroup) ist, deaktivieren Sie ALUA aufdem NetApp-Array.
EqualLogic	Stellen Sie sicher, dass die ARP-Weiterleitung auf den Hardware-iSCSI-Adaptern aktiviert ist.
LeftHand	Stellen Sie sicher, dass die ARP-Weiterleitung auf den Hardware-iSCSI-Adaptern aktiviert ist.
ESX/ESXi-Konfiguration	Stellen Sie die folgenden erweiterten Einstellungen für den ESX/ESXi-Host ein: ■ Setzen Sie **[Disk.UseLunReset]** auf **[1]** . ■ Setzen Sie **[Disk.UseDeviceReset]** auf **[0]** . Für alle LUNs, die geclusterte Festplatten für Aktiv/Passiv-Arrays hosten, muss eine Multipathing-Richtlinie des Typs **[Zuletzt verwendet]** gesetzt werden. Für LUNs auf Aktiv/Aktiv-Arrays kann eine Multipathing-Richtlinie des Typs **[Zuletzt verwendet]** oder **[Fest]** festgelegt werden. Lassen Sie ARP-Umleitung zu, wenn das Speichersystem transparentes Failover unterstützt.

VMware vSphere-Befehlszeilenschnittstelle

B

In den meisten Fällen eignet sich der vSphere-Client sehr gut zur Überwachung eines ESX/ESXi-Hosts, der mit einem SAN-Speicher verbunden ist. Fortgeschrittene Benutzer möchten hin und wieder möglicherweise einige VMware vSphere CLI (Command-Line Interface)-Befehle für zusätzliche Details verwenden.

Weitere Informationen finden Sie im Handbuch *vSphere Command-Line Interface Installation and Scripting Guide*.

Dieser Anhang behandelt die folgenden Themen:

- „resxtop-Befehl“, auf Seite 113
- „vicfg-iscsi-Befehl“, auf Seite 113
- „vicfg-mpath-Befehl“, auf Seite 113
- „esxcli corestorage claimrule-Befehl“, auf Seite 114
- „vmkping-Befehl“, auf Seite 114

resxtop-Befehl

Der `resxtop`-Befehl bietet einen sehr ausführlichen Überblick darüber, wie ESX/ESXi Ressourcen in Echtzeit nutzt.

Ausführliche Informationen zu `resxtop` finden Sie in den Handbüchern *Handbuch zur Ressoucenverwaltung* und *vSphere Command-Line Interface Installation and Scripting Guide*.

vicfg-iscsi-Befehl

Mit dem Befehl `vicfg-iscsi`-Befehl können Sie Software- oder Hardware-iSCSI auf ESX/ESXi-Hosts konfigurieren sowie CHAP-Parameter und ein iSCSI-Netzwerk einrichten.

Weitere Informationen hierzu finden Sie in den Handbüchern *vSphere Command-Line Interface Installation and Scripting Guide* und *vSphere Command-Line Interface Reference*.

vicfg-mpath-Befehl

Verwenden Sie den `vicfg-mpath`-Befehl, um Informationen zu Speichergeräten, Pfaden und Multipathing-Plug-Ins anzuzeigen.

Weitere Informationen hierzu finden Sie in den Handbüchern *vSphere Command-Line Interface Installation and Scripting Guide* und *vSphere Command-Line Interface Reference*.

esxcli corestorage claimrule-Befehl

Verwenden Sie den Befehl `esxcli corestorage claimrule`, um Beanspruchungsregeln zu verwalten. Beanspruchungsregeln legen fest, welches Multipathing-Modul Pfade zu einem bestimmten Geräten beanspruchen und das Gerät verwalten sollten.

Weitere Informationen hierzu finden Sie in den Handbüchern *vSphere Command-Line Interface Installation and Scripting Guide* und *vSphere Command-Line Interface Reference*.

vmkping-Befehl

Der Befehl `vmkping` ermöglicht die Verifizierung der VMkernel-Netzwerkkonfiguration.

Anwendungsbeispiel:

```
vmkping [Optionen] [Host|IP–Adresse]
```

Tabelle B-1. vmkping-Optionen

Option	Beschreibung
–6	Verwenden von IPv6 - ICMPv6-Echoanforderung.
–4	Verwenden von IPv4 (Standard).
–I	Ausgehende Schnittstelle - für IPv6-Bereich.
–D	Debug-Modus des VMkernel-TCP-Stapels.
–c ***Anzahl***	Legt die Anzahl an Paketen fest.
–I ***Intervall***	Legt das Intervall fest.
–s ***Größe***	Legt die Sendegröße fest.
–d	Setzt das DF-Bit auf IPv4-Pakete.
–v	Ausführlich.

Verwalten von Multipathing-Modulen und Hardwarebeschleunigungs-Plug-Ins

C

Verwenden Sie die vSphere CLI zur Verwaltung von PSA-Multipathing-Plug-Ins und Hardwarebeschleunigungs-Plug-Ins.

Dieser Anhang behandelt die folgenden Themen:

- „Verwalten von Speicherpfaden und Multipathing-Plug-Ins“, auf Seite 115
- „Verwalten des Hardwarebeschleunigungsfilters und der Hardwarebeschleunigungs-Plug-Ins“, auf Seite 122
- „esxcli corestorage claimrule - Optionen“, auf Seite 125

Verwalten von Speicherpfaden und Multipathing-Plug-Ins

Mithilfe der vSphere-CLI können Sie die PSA-Multipathing-Plug-Ins und die ihnen zugewiesenen Speicherpfade verwalten.

Sie können alle auf Ihrem Host verfügbaren Multipathing-Plug-Ins anzeigen. Sie können alle Drittanbieter-MPPs sowie die NMP und SATPs Ihres Hosts auflisten und die Pfade überprüfen, die sie beanspruchen. Sie können ebenfalls neue Pfade festlegen und angeben, welches Multipathing-Plug-In die Pfade beansprucht.

Informationen zu Befehlen für die PSA-Verwaltung finden Sie in den Handbüchern *vSphere Command-Line Interface Installation and Scripting Guide* und *vSphere Command-Line Interface Reference*.

Auflisten von Multipathing-Beanspruchungsregeln für den Host

Verwenden Sie die vSphere-CLI, um die verfügbaren Multipathing-Beanspruchungsregeln aufzulisten.

Beanspruchungsregeln geben an, welches Multipathing-Plug-In, NMP oder Drittanbieter-MPP einen vorhandenen physischen Pfad verwalten. Jede Beanspruchungsregel gibt einen Satz an Pfaden basierend auf folgenden Parametern an:

- Hersteller-/Modellzeichenfolgen
- Übertragung wie zum beispiel SATA, IDE, Fibre-Channel usw.
- Adapter, Ziel- oder LUN-Speicherort
- Gerätetreiber, zum Beispiel Mega-RAID

Vorgehensweise

- Verwenden Sie den Befehl `esxcli corestorage claimrule list --claimrule-class=MP`, um die Multipathing-Beanspruchungsregeln aufzulisten.

  Beispiel C-1 zeigt die Ausgabe des Befehls.

Beispiel C-1. Beispielausgabe des Befehls esxcli corestorage claimrule list

```
Rule Class  Rule   Class    Type       Plugin     Matches
MP          0      runtime  transport  NMP        transport=usb
MP          1      runtime  transport  NMP        transport=sata
MP          2      runtime  transport  NMP        transport=ide
MP          3      runtime  transport  NMP        transport=block
MP          4      runtime  transport  NMP        transport=unknown
MP          101    runtime  vendor     MASK_PATH  vendor=DELL model=Universal Xport
MP          101    file     vendor     MASK_PATH  vendor=DELL model=Universal Xport
MP          200    runtime  vendor     MPP_1      vendor=NewVend model=*
MP          200    file     vendor     MPP_1      vendor=NewVend model=*
MP          201    runtime  location   MPP_2      adapter=vmhba41 channel=* target=* lun=*
MP          201    file     location   MPP_2      adapter=vmhba41 channel=* target=* lun=*
MP          202    runtime  driver     MPP_3      driver=megaraid
MP          202    file     driver     MPP_3      driver=megaraid
MP          65535  runtime  vendor     NMP        vendor=* model=*
```

Dieses Beispiel zeigt Folgendes an:

- Das NMP beansprucht alle mit den Speichergeräten verbundenen Pfade, die USB-, SATA-, IDE- und Block SCSI-Übertragung verwenden.
- Das MASK_PATH-Modul beansprucht standardmäßig alle Pfade, die SCSI-Anfragedaten mit der Herstellerzeichenfolge „DELL“ und einer Modellzeichenfolge „Universal Xport“ zurückgeben. Das MASK_PATH-Modul wird zum Maskieren von Pfaden gegenüber Ihrem Host verwendet.
- Das MPP_1-Modul beansprucht alle mit einem beliebigen Modell des NewVend-Speicher-Arrays verbundenen Pfade.
- Das MPP_3-Modul beansprucht die Pfade zu Speichergeräten, die vom Mega-RAID-Gerätetreiber gesteuert werden.
- Alle nicht in den vorherigen Regeln beschriebenen Pfade werden von NMP beansprucht.
- Die Spalte „Rule Class“ der Ausgabe beschreibt die Kategorie einer Beanspruchungsregel. Sie kann MP (Multipathing-Plug-In), Filter oder VAAI sein.
- Die Class-Spalte zeigt, welche Regeln definiert und welche geladen sind. Der Parameter `file` in der Class-Spalte gibt an, dass die Regel definiert ist. Der Parameter `runtime` gibt an, dass die Regel in Ihr System geladen wurde. Damit eine benutzerdefinierte Regel aktiv wird, müssen zwei Zeilen in der selben Regelnummer enthalten sein. Eine Zeile für die Regel mit dem Parameter `file` und eine Zeile mit `runtime`. Einige Regeln mit niedrigen Nummern verfügen lediglich über eine Zeile mit der Class-Spalte `runtime`. Dies sind vom System festgelegte Beanspruchungsregeln, die nicht geändert werden können.

Anzeigen von Multipathing-Modulen

Sie verwenden die vSphere-CLI, um alle im System geladenen Mutipathing-Module aufzulisten. Multipathing-Module verwalten physische Pfade, die Ihren Host mit Speicher verbinden.

Vorgehensweise

- Führen Sie den folgenden Befehl aus, um alle Mutipathing-Module aufzulisten:

  `esxcli corestorage plugin list –-plugin–class=MP`

Dieser Befehl gibt mindestens das NMP und die MASK_PATH-Module zurück. Wenn Drittanbieter-MPPs geladen wurden, werden diese ebenfalls aufgelistet.

Anzeigen von SATPs für den Host

Sie verwenden die vSphere-CLI, um alle in das System geladenen VMware NMP SATPs aufzulisten.

Vorgehensweise

- Führen Sie den folgenden Befehl aus, um alle VMware SATPs aufzulisten.

  ```
  esxcli nmp satp list
  ```

Für jedes SATP zeigt der Befehl Informationen an, die den Typ des Speicher-Arrays oder Systems, das dieses SATP unterstützt, sowie das Standard-PSP für alle LUNs anzeigt, die dieses SATP verwenden.

Beachten Sie Folgendes:

- Wenn dem Gerät anhand der Beanspruchungsregeln kein SATP zugewiesen ist, lautet das Standard-SATP für iSCSI- oder FC-Geräte VMW_SATP_DEFAULT_AA. Das Standard-PSP lautet VMW_PSP_FIXED.
- Wenn VMW_SATP_ALUA einem bestimmten Speichergerät zugewiesen ist, dieses Gerät ALUA jedoch nicht erkennt, gibt es für dieses Gerät keine Beanspruchungsregelübereinstimmung. Das Gerät wird in diesem Fall vom Standard-SATP gemäß dem Übertragungstyp des Geräts beansprucht.
- Das Standard-PSP für alle von VMW_SATP_ALUA beanspruchten Geräte lautet VMW_PSP_MRU. Das VMW_PSP_MRU wählt wie vom VMW_SATP_ALUA angegeben einen aktiven/optimierten Pfad oder einen aktiven/nicht optimierten Pfad aus, falls kein aktiver/optimierter Pfad vorhanden ist. Dieser Pfad wir so lange verwendet, bis ein besserer Pfad verfügbar ist (MRU). Wenn das VMW_PSP_MRU derzeit einen aktiven/nicht optimierten Pfad verwendet und ein aktiver/optimierter Pfad verfügbar wird, wechselt das VMW_PSP_MRU vom aktuellen Pfad zum aktiven/optimierten Pfad,

Anzeigen von NMP-Speichergeräten

Sie verwenden die vSphere-CLI, um all von VMware NMP gesteuerten Speichergeräte aufzulisten und mit diesen Geräten verbundene SATP- und PSP-Informationen anzuzeigen.

Vorgehensweise

1. Führen Sie den folgenden Befehl aus, um alle Speichergeräte aufzulisten:

   ```
   esxcli nmp device list
   ```

2. Führen Sie zum Anzeigen von Informationen für ein bestimmtes Gerät den folgenden Befehl aus:

   ```
   esxcli nmp device list –d device_ID
   ```

Hinzufügen von Multipathing-Beanspruchungsregeln

Verwenden Sie die vSphere-CLI, um eine neue Multipathing-PSA-Beanspruchungsregel zum Satz an Beanspruchungsregeln im System hinzuzufügen. Zur Aktivierung der neuen Beanspruchungsregeln müssen Sie diese zunächst definieren und in Ihr System laden.

Sie fügen eine neue PSA-Beanspruchungsregel beispielsweise hinzu, wenn Sie ein neues MPP (Multipathing-Plug-In) laden und festlegen müssen, welche Pfade dieses Modul beanspruchen soll. Möglicherweise müssen Sie eine Beanspruchungsregel erstellen, wenn Sie neue Pfade hinzufügen, die von einem vorhandenen MPP beansprucht werden sollen.

Vorsicht Vermeiden Sie beim erstellen von neuen Beanspruchungsregeln Situationen, in denen verschiedene physische Pfade zu derselben LUN von verschiedenen MPPs beansprucht werden. Wenn es sich bei einem MPP nicht um MASK_PATH MPP handelt, ruft diese Konfiguration Leistungsprobleme hervor.

Vorgehensweise

1 Führen Sie zum Definieren einer neuen Beanspruchungsregel auf der vSphere-CLI den folgenden Befehl aus:

```
esxcli corestorage claimrule add
```

Weitere Informationen darüber, welche Optionen für die Ausführung des Befehls erforderlich sind, finden Sie unter „esxcli corestorage claimrule - Optionen“, auf Seite 125.

2 Führen Sie zum Laden der neuen Beanspruchungsregel in Ihr System den folgenden Befehl aus:

```
esxcli corestorage claimrule load
```

Dieser Befehl lädt alle neu erstellten Multipathing-Beanspruchungsregeln aus der Konfigurationsdatei Ihres Systems.

Beispiel C-2. Definieren von Multipathing-Beanspruchungsregeln

- Fügen Sie Regel Nummer 500 hinzu, um alle Pfade mit der Modellzeichenfolge „NewMod“ und der Herstellerzeichenfolge „NewVend“ für das NMP-Plug-In zu beanspruchen.

  ```
  # esxcli corestorage claimrule add –r 500 –t vendor –V NewVend –M NewMod –P NMP
  ```

  Wenn Sie die Beanspruchungsregel laden und den Befehl **`esxcli corestorage claimrule list`** ausführen, wird anschließend die neue Beanspruchungsregel in der Liste angezeigt.

  Hinweis Die beiden Zeilen für die Beanspruchungsregel mit der Klasse `runtime` und der Klasse `file` geben an, dass die neue Beanspruchungsregel in das System geladen wurde und aktiv ist.

  ```
  Rule Class  Rule   Class    Type       Plugin     Matches
  MP          0      runtime  transport  NMP        transport=usb
  MP          1      runtime  transport  NMP        transport=sata
  MP          2      runtime  transport  NMP        transport=ide
  MP          3      runtime  transport  NMP        transport=block
  MP          4      runtime  transport  NMP        transport=unknown
  MP          101    runtime  vendor     MASK_PATH  vendor=DELL model=Universal Xport
  MP          101    file     vendor     MASK_PATH  vendor=DELL model=Universal Xport
  MP          500    runtime  vendor     NMP        vendor=NewVend model=NewMod
  MP          500    file     vendor     NMP        vendor=NewVend model=NewMod
  ```

- Fügen Sie Regel Nummer 321 hinzu, um den Pfad auf Adapter „vmhba0“, Kanal „0“, Ziel „0“, LUN „0“ für das NMP-Plug-In zu beanspruchen.

  ```
  # esxcli corestorage claimrule add –r 321 –t location –A vmhba0 –C 0 –T 0 –L 0 –P NMP
  ```

- Fügen Sie Regel Nummer 1015 hinzu, um alle Pfade zu beanspruchen, die von Fibre-Channel-Adaptern für das NMP-Plug-In zur Verfügung gestellt werden.

  ```
  # esxcli corestorage claimrule add –r 1015 –t transport –R fc –P NMP
  ```

- Fügen Sie eine Regel mit einer vom System zugewiesenen Regel-ID hinzu, um alle Pfade zu beanspruchen, die von Adaptern des Fibre-Channel-Typs für das NMP-Plug-In zur Verfügung gestellt werden.

  ```
  # esxcli corestorage claimrule add ––autoassign –t transport –R fc –P NMP
  ```

Löschen von Multipathing-Beanspruchungsregeln

Anhand der vSphere-CLI können Sie eine Multipathing-PSA-Beanspruchungsregel aus dem Beanspruchungsregelsatz auf dem System entfernen.

Vorgehensweise

1 Führen Sie zum Löschen einer Beanspruchungsregel aus dem Satz von Beanspruchungsregeln den folgenden Befehl aus.

```
esxcli corestorage claimrule delete –r claimrule_ID
```

Weitere Informationen darüber, welche Optionen für die Ausführung des Befehls erforderlich sind, finden Sie unter „esxcli corestorage claimrule - Optionen“, auf Seite 125.

Hinweis Die PSA-Beanspruchungsregel 101 maskiert standardmäßig Pseudo-Array-Geräte von Dell. Löschen Sie diese Regel nur, wenn die Maskierung dieser Geräte aufgehoben werden soll.

2 Löschen Sie die Beanspruchungsregel aus dem ESX/ESXi-System.

```
esxcli corestorage claimrule load
```

Maskieren von Pfaden

Sie können verhindern, dass der ESX/ESXi-Host auf Speichergeräte oder LUNs zugreift oder einzelne Pfade zu einer LUN verwendet. Verwenden Sie vSphere-CLI-Befehle, um die Pfade zu maskieren.

Beim Maskieren von Pfaden können Sie Beanspruchungsregeln erstellen, die das MASK_PATH-Plug-In bestimmten Pfaden zuordnen.

Vorgehensweise

1 Prüfen Sie, welche die nächste verfügbare Regel-ID ist:

```
esxcli corestorage claimrule list
```

Die zur Maskierung von Pfaden verwendeten Beanspruchungsregeln sollten über Regel-IDs im Bereich 101-200 verfügen. Wenn der Befehl zeigt, dass die Regeln 101 und 102 bereits vorhanden sind, können Sie festlegen, dass der Regel die Nummer 103 hinzugefügt wird.

2 Weisen Sie das MASK_PATH-Plug-In einem Pfad zu, indem Sie eine neue Beanspruchungsregel für das Plug-In erstellen.

```
esxcli corestorage claimrule add –P MASK_PATH
```

Weitere Informationen zu Befehlszeilenoptionen finden Sie unter „esxcli corestorage claimrule - Optionen“, auf Seite 125.

3 Laden Sie die MASK_PATH-Beanspruchungsregel in Ihr System.

```
esxcli corestorage claimrule load
```

4 Prüfen Sie, ob die MASK_PATH-Beanspruchungsregel ordnungsgemäß hinzugefügt wurde.

```
esxcli corestorage claimrule list
```

5 Falls für den maskierten Pfad eine Beanspruchungsregel vorhanden ist, entfernen Sie die Regel.

```
esxcli corestorage claiming unclaim
```

6 Führen Sie die Pfadbeanspruchungsregeln aus.

```
esxcli corestorage claimrule run
```

Nach dem Zuweisen des MASK_PATH-Plug-Ins zu einem Pfad verliert der Pfadstatus an Bedeutung und wird nicht länger vom Host verwaltet. Befehle, die Informationen zum maskierten Pfad bereitstellen, zeigen den Pfadstatus als nicht verfügbar (dead) an.

Beispiel C-3. Maskieren einer LUN

Im vorliegenden Beispiel wird die LUN 20 auf den Zielen T1 und T2 maskiert, auf die über die Speicheradapter vmhba2 und vmhba3 zugegriffen wird.

1 `#esxcli corestorage claimrule list`

2
```
#esxcli corestorage claimrule add –P MASK_PATH –r 109 –t location –A vmhba2 –C 0 –T 1 –L 20
#esxcli corestorage claimrule add –P MASK_PATH –r 110 –t location –A vmhba3 –C 0 –T 1 –L 20
#esxcli corestorage claimrule add –P MASK_PATH –r 111 –t location –A vmhba2 –C 0 –T 2 –L 20
#esxcli corestorage claimrule add –P MASK_PATH –r 112 –t location –A vmhba3 –C 0 –T 2 –L 20
```

3 `# esxcli corestorage claimrule load`

4 `#esxcli corestorage claimrule list`

5
```
#esxcli corestorage claiming unclaim –t location –A vmhba2
#esxcli corestorage claiming unclaim –t location –A vmhba3
```

6 `# esxcli corestorage claimrule run`

Aufheben der Maskierung von Pfaden

Falls es erforderlich ist, dass der Host Zugriff auf das maskierte Speichergerät erhält, müssen Sie die Maskierung der Pfade zu diesem Gerät aufheben.

Vorgehensweise

1 Löschen Sie die Beanspruchungsregel „MASK_PATH“.

esxcli *Verbindungsoptionen* corestorage claimrule delete –r *Regelnummer*

2 Stellen Sie sicher, dass die Beanspruchungsregel ordnungsgemäß gelöscht wurde.

esxcli *Verbindungsoptionen* corestorage claimrule list

3 Laden Sie die Pfadbeanspruchungsregeln aus der Konfigurationsdatei neu in den VMkernel.

esxcli *Verbindungsoptionen* corestorage claimrule load

4 Führen Sie den Befehl `esxcli corestorage claiming unclaim` für jeden Pfad eines maskierten Speichergeräts aus.

Beispiel:

esxcli *Verbindungsoptionen* corestorage claiming unclaim –t location –A vmhba0 –C 0 –T 0 –L 149

5 Führen Sie die Pfadbeanspruchungsregeln aus.

esxcli *Verbindungsoptionen* corestorage claimrule run

Ihr Host hat jetzt Zugriff auf das zuvor maskierte Speichergerät.

Definieren von NMP SATP-Regeln

Die NMP SATP-Beanspruchungsregeln geben an, welches SATP ein bestimmtes Speichergerät verwalten sollen. Normalerweise ist es nicht erforderlich, NMP SATP-Regeln zu ändern. Falls doch, verwenden Sie die vSphere-CLI, um eine neue Regel zu Liste der Beanspruchungsregeln für das angegebene SATP hinzuzufügen.

Beim Installieren eines Drittanbieter-SATP für eine bestimmtes Speicher-Array müssen Sie unter Umständen eine SATP-Regel erstellen.

Vorgehensweise

1 Führen Sie zum Hinzufügen einer Beanspruchungsregel für ein bestimmtes SATP den Befehl `esxcli nmp satp addrule` aus. Der Befehl verfügt über die folgenden Optionen.

Option	Beschreibung
-c|--claim-option	Legt die Zeichenfolge der Beanspruchungsoption beim Hinzufügen einer SATP-Beanspruchungsregel fest. Die Zeichenfolge wird an das SATP übergeben, wenn das SATP einen Pfad beansprucht. Der Inhalt einer Zeichenfolge und dessen Verarbeitung durch ein SATP sind eindeutig für jedes SATP. Einige SATPs unterstützen beispielsweise die Beanspruchungsregelzeichenfolgen `tpgs_on` und `tpgs_off`. Wenn `tpgs_on` angegeben ist, beansprucht SATP den Pfad nur, wenn die ALUA Target Port Group-Unterstützung auf dem Speichergerät aktiviert ist.
-e|--description	Legt die Beschreibung der Beanspruchungsregel beim Hinzufügen einer SATP-Beanspruchungsregel fest.
-d|--device	Legt das Gerät beim Hinzufügen von SATP-Beanspruchungsregeln fest. Geräteregeln und Anbieter/Modell- sowie Treiberregeln schließen sich gegenseitig aus.
-D|--driver	Legt die Treiberzeichenfolge beim Hinzufügen einer SATP-Beanspruchungsregel fest. Treiberregeln und Anbieter/Modell-Regeln schließen sich gegenseitig aus.
-f|--force	Erzwingt, dass Beanspruchungsregeln Gültigkeitsprüfungen ignorieren und die Regel in jedem Fall installieren.
-h|--help	Zeigt die Hilfemeldung an.
-M|--model	Legt die Modellzeichenfolge beim Hinzufügen einer SATP-Beanspruchungsregel fest. Anbieter/Modell-Regeln und Treiberregeln schließen sich gegenseitig aus.
-o|--option	Legt die Optionszeichenfolge beim Hinzufügen einer SATP-Beanspruchungsregel fest.
-P|--psp	Legt das Standard-PSP für die SATP-Beanspruchungsregel fest.
-O|--psp-option	Legt die PSP-Optionen für die SATP-Beanspruchungsregel fest.
-s|--satp	Das SATP, für das eine neue Regel hinzugefügt wird.
-R|--transport	Legt die Zeichenfolge für den Beanspruchungs-Transporttyp beim Hinzufügen einer SATP-Beanspruchungsregel fest.
-V|--vendor	Legt die Herstellerzeichenfolge beim Hinzufügen von SATP-Beanspruchungsregeln fest. Anbieter/Modell-Regeln und Treiberregeln schließen sich gegenseitig aus.

HINWEIS Beim Durchsuchen der SATP-Regeln zur Ermittlung eines SATP für ein vorhandenes Gerät werden zunächst die Treiberregeln vom NMP durchsucht. Ist die Suche dort nicht erfolgreich, werden die Hersteller- bzw. Modellregeln und anschließend die Übertragungsregeln durchsucht. Werden immer noch keine Ergebnisse angezeigt, wählt NMP ein Standard-SATP für das Gerät aus.

2 Führen Sie zum Löschen einer Regel aus der Liste der Beanspruchungsregeln für die angegebene SATP folgenden Befehl aus.

Sie können diesen Befehl mit denselben Optionen ausführen, die Sie für die Regel zum Hinzufügen verwendet haben.

```
esxcli nmp satp deleterule
```

3 Starten Sie Ihren Host neu.

Beispiel C-4. Definieren einer NMP SATP-Regel

Der folgende Beispielbefehl ordnet das VMW_SATP_INV-Plug-In zu, um Speicher-Arrays mit der Herstellerzeichenfolge NewVend und der Modellzeichenfolge NewMod zu verwalten.

```
# esxcli nmp satp addrule –V NewVend –M NewMod –s VMW_SATP_INV
```

Wenn Sie den Befehl **`esxcli nmp satp listrules –s VMW_SATP_INV`** ausführen, wird die neue Regel der Regelliste VMW_SATP_INV hinzugefügt.

Verwalten des Hardwarebeschleunigungsfilters und der Hardwarebeschleunigungs-Plug-Ins

Der Hardwarebeschleunigungs- oder VAAI-Filter wird in Kombination mit herstellerspezifischen VAAI-Plug-Ins an Speichergeräte angehängt, die die Hardwarebeschleunigung unterstützen. Mithilfe der vSphere-CLI können Sie den VAAI-Filter und die VAAI-Plug-Ins anzeigen und bearbeiten.

Anzeigen des Hardwarebeschleunigungs-Filters

Verwenden Sie die vSphere-CLI, um den Hardwarebeschleunigungs- oder VAAI-Filter anzuzeigen, der derzeit in Ihrem System geladen ist.

Vorgehensweise

- Führen Sie den Befehl `esxcli corestorage plugin list –-plugin–class=Filter` aus.

Die Ausgabe dieses Befehls lautet in etwa wie folgt:

```
Plugin name  Plugin class
VAAI_FILTER  Filter
```

Anzeigen von Hardwarebeschleunigungs-Plug-Ins

Verwenden Sie die vSphere-CLI, um die derzeit in Ihrem System geladenen Hardwarebeschleunigungs-Plug-Ins, auch VAAI-Plug-Ins genannt, anzuzeigen.

Vorgehensweise

- Führen Sie den Befehl `esxcli corestorage plugin list –-plugin–class=VAAI` aus.

Die Ausgabe dieses Befehls lautet in etwa wie folgt:

```
Plugin name         Plugin class
VMW_VAAIP_EQL       VAAI
VMW_VAAIP_NETAPP    VAAI
VMW_VAAIP_CX        VAAI
```

Überprüfen des Hardwarebeschleunigungs-Status eines Speichergeräts

Verwenden Sie die vSphere-CLI, um den Hardwarebeschleunigungs-Unterstützungsstatus eines bestimmten Speichergeräts zu überprüfen. Dieser Befehl hilft auch festzustellen, welcher VAAI-Filter mit dem Gerät verbunden ist.

Vorgehensweise

- Führen Sie den Befehl **`esxcli corestorage device list –-d`** ***`Geräte–ID`*** aus.

Die Ausgabe zeigt den Hardwarebeschleunigung- oder VAAI-Status an, der „Unbekannt“, „Unterstützt“ oder „Nicht unterstützt“ lauten kann. Wenn das Gerät die Hardwarebeschleunigung unterstützt, listet die Ausgabe auch den an das Gerät angehängten VAAI-Filter auf.

```
# esxcli corestorage device list --d naa.60a98000572d43595a4a52644473374c
naa.60a98000572d43595a4a52644473374c
 Anzeigename: NETAPP Fiberkanal-Datenträger(naa.60a98000572d43595a4a52644473374c)
 Größe: 20480
 Gerätetyp: Direktzugriff
 Multipath Plug-In: NMP
 Devfs-Pfad: /vmfs/devices/disks/naa.60a98000572d43595a4a52644473374c
 Hersteller: NETAPP
 Modell: LUN
 Revision: 8000
 SCSI-Ebene: 4
 Ist Pseudo: false
 Status: an
 Ist RDM aktiv: true
 Ist lokal: false
 Ist entfernbar: false
 Angehängte Filter: VAAI_FILTER
 VAAI-Status: Unterstützt
 Weitere UIDs: vml.020003000060a98000572d43595a4a52644473374c4c554e202020
```

Anzeigen des Hardwarebeschleunigungs-Plug-Ins für ein Gerät

Verwenden Sie die vSphere-CLI, um das Hardwarebeschleunigungs- oder VAAI-Plug-In anzuzeigen, das an ein Speichergerät angehängt ist, das die Hardwarebeschleunigung unterstützt.

Vorgehensweise

- Führen Sie den Befehl **`esxcli vaai device list --d`** ***`Geräte-ID`*** aus.

  Beispiel:

  ```
  # esxcli vaai device list -d naa.6090a028d00086b5d0a4c44ac672a233
  naa.6090a028d00086b5d0a4c44ac672a233
   Device Display Name: EQLOGIC iSCSI Disk (naa.6090a028d00086b5d0a4c44ac672a233)
   VAAI Plugin Name: VMW_VAAIP_EQL
  ```

Auflisten der Hardwarebeschleunigungs-Beanspruchungsregeln

Für jedes Speichergerät, das die Hardwarebeschleunigungs-Funktionalität unterstützt, geben die Beanspruchungsregeln den Hardwarebeschleunigungs-Filter und das Hardwarebeschleunigungs-Plug-In zum Verwalten dieses Speichergeräts an. Sie können die vSphere-CLI dazu verwenden, die Beanspruchungsregeln für den Hardwarebeschleunigungs-Filter und das Hardwarebeschleunigungs-Plug-In aufzulisten.

Vorgehensweise

1 Führen Sie zum Auflisten der Filter-Beanspruchungsregeln den Befehl `esxcli corestorage claimrule list --claimrule-class=Filter` aus.

In diesem Beispiel geben die Filter-Beanspruchungsregeln Geräte an, die durch den Filter VAAI_FILTER beansprucht werden sollten.

```
# esxcli corestorage claimrule list --claimrule-class=Filter
Rule Class   Rule   Class   Type   Plugin      Matches
Filter       65430  runtime vendor VAAI_FILTER vendor=EMC model=SYMMETRIX
Filter       65430  file    vendor VAAI_FILTER vendor=EMC model=SYMMETRIX
Filter       65431  runtime vendor VAAI_FILTER vendor=DGC model=*
Filter       65431  file    vendor VAAI_FILTER vendor=DGC model=*
```

2 Führen Sie zum Auflisten der VAAI-Plug-In-Beanspruchungsregeln den Befehl `esxcli corestorage claimrule list --claimrule-class=VAAI` aus.

In diesem Beispiel geben die VAAI-Beanspruchungsregeln Geräte an, die durch ein bestimmtes VAAI-Plug-In beansprucht werden sollten.

```
esxcli corestorage claimrule list --claimrule-class=VAAI
Rule Class   Rule   Class   Type    Plugin         Matches
VAAI         65430  runtime vendor  VMW_VAAIP_SYMM vendor=EMC model=SYMMETRIX
VAAI         65430  file    vendor  VMW_VAAIP_SYMM vendor=EMC model=SYMMETRIX
VAAI         65431  runtime vendor  VMW_VAAIP_CX   vendor=DGC model=*
VAAI         65431  file    vendor  VMW_VAAIP_CX   vendor=DGC model=*
```

Hinzufügen von Hardwarebeschleunigungs-Beanspruchungsregeln

Um die Hardwarebeschleunigung für ein neues Array zu konfigurieren, müssen Sie zwei Beanspruchungsregeln hinzufügen, eine für den VAAI-Filter und eine weitere für das VAAI-Plug-In. Damit die neuen Beanspruchungsregeln aktiv sind, definieren Sie zuerst die Regeln und laden Sie sie anschließend in Ihr System.

Vorgehensweise

1 Definieren Sie eine neue Beanspruchungsregel für den VAAI-Filter, indem Sie den Befehl `esxcli corestorage claimrule add --claimrule-class=Filter --plugin=VAAI_FILTER` ausführen.

Weitere Informationen darüber, welche Optionen für die Ausführung des Befehls erforderlich sind, finden Sie unter „esxcli corestorage claimrule - Optionen“, auf Seite 125.

2 Definieren Sie eine neue Beanspruchungsregel für das VAAI-Plug-In, indem Sie den Befehl `esxcli corestorage claimrule add --claimrule-class=VAAI` ausführen.

3 Laden Sie beide Beanspruchungsregeln, indem Sie die folgenden Befehle verwenden:

```
esxcli corestorage claimrule load --claimrule-class=Filter
```

```
esxcli corestorage claimrule load --claimrule-class=VAAI
```

4 Führen Sie die VAAI-Filter-Beanspruchungsregel aus, indem Sie den Befehl `esxcli corestorage claimrule run --claimrule-class=Filter` verwenden.

HINWEIS Es müssen nur die Regeln der Klasse „Filter“ ausgeführt werden. Wenn der VAAI-Filter ein Gerät beansprucht, findet er automatisch das richtige VAAI-Plug-In, das angehängt werden muss.

Beispiel C-5. Definieren von Hardwarebeschleunigungs-Beanspruchungsregeln

Verwenden Sie die folgende Befehlsfolge, um die Hardwarebeschleunigung für IBM-Arrays mithilfe des VMW_VAAI_T10-Plug-Ins zu konfigurieren:

```
# esxcli corestorage claimrule add --claimrule-class=Filter --plugin=VAAI_FILTER --type=vendor --vendor=IBM --autoassign
# esxcli corestorage claimrule add --claimrule-class=VAAI --plugin=VMW_VAAI_T10 --type=vendor --vendor=IBM --autoassign
# esxcli corestorage claimrule load --claimrule-class=Filter
# esxcli corestorage claimrule load --claimrule-class=VAAI
# esxcli corestorage claimrule run --claimrule-class=Filter
```

Löschen von Hardwarebeschleunigungs-Beanspruchungsregeln

Anhand der vSphere-CLI können Sie vorhandene Hardwarebeschleunigungs-Beanspruchungsregeln löschen.

Vorgehensweise

- Verwenden Sie die folgenden Befehle:

```
esxcli corestorage claimrule delete -r claimrule_ID --claimrule-class=Filter
```

```
esxcli corestorage claimrule delete -r claimrule_ID --claimrule-class=VAAI
```

esxcli corestorage claimrule - Optionen

Für die Ausführung bestimmter `esxcli corestorage claimrule`-Befehle, z. B. zum Hinzufügen neuer Beanspruchungsregeln, zum Entfernen der Regeln oder zum Maskieren von Pfaden, müssen Sie mehrere Optionen angeben.

Tabelle C-1. esxcli corestorage claimrule - Optionen

Option	Beschreibung
-A|--adapter	Gibt den Adapter der Pfade an, der für diesen Vorgang verwendet werden soll.
-u|--autoassign	Das System weist automatisch eine Regel-ID zu.
-C|--channel	Gibt den Kanal der Pfade an, der für diesen Vorgang verwendet werden soll.
-c|--claimrule-class	Gibt die Beanspruchungsregel-Klasse an, die für diesen Vorgang verwendet werden soll. Gültige Werte sind: MP, Filter, VAAI
-d|--device	Gibt die Geräte-UID an, die für diesen Vorgang verwendet werden soll.
-D|--driver	Gibt den Treiber der Pfade an, der für diesen Vorgang verwendet werden soll.

Tabelle C-1. esxcli corestorage claimrule - Optionen (Fortsetzung)

Option	Beschreibung
-f|--force	Erzwingt, dass Beanspruchungsregeln Gültigkeitsprüfungen ignorieren und die Regel in jedem Fall installieren.
-h|--help	Zeigt die Hilfemeldung an.
-L|--lun	Gibt die LUN der Pfade an, die für diesen Vorgang verwendet werden soll.
-M|--model	Gibt das Modell der Pfade an, das für diesen Vorgang verwendet werden soll.
-P|--plugin	Gibt an, welches PSA-Plug-In für diesen Vorgang verwendet werden soll.
-r|--rule	Gibt die Beanspruchungsregel-ID an, die für diesen Vorgang verwendet werden soll.
-T|--target	Gibt das Ziel der Pfade an, das für diesen Vorgang verwendet werden soll.
-R|--transport	Gibt den Transport der Pfade an, der für diesen Vorgang verwendet werden soll. Gültige Werte sind: block, fc, iscsi, iscsivendor, ide, sas, sata, usb, parallel, unknown.
-t|--type	Gibt an, welcher Abgleichstyp für „claim/unclaim“ oder „claimrule“ verwendet wird. Gültige Werte sind: vendor, location, driver, transport, device.
-V|--vendor	Gibt den Anbieter der Pfade an, das für diesen Vorgang verwendet werden soll.

Index

Symbole

* neben dem Pfad **90**

A

abhängige Hardware iSCSI
  Konfigurations-Workflow **35**
  Überlegungen **36**
  Überprüfen von Adaptern **36**
  und zugeordnete Netzwerkkarten **36**
Adaptives Modell **20**
Aktiv/Aktiv-Festplatten-Arrays, Verwalten von Pfaden **93**
Aktiv/Passiv-Festplatten-Arrays
  Pfad-Thrashing **100**
  Verwalten von Pfaden **93**
Aktueller Multipathing-Status **90**
Anwendungen, Mehrschichtig **104**
Anwendungsbeispiele **15**
Anzeigeprobleme **84**
Architektur des im Betrieb austauschbaren Speichers **22**
Array-basierte Lösung **104**
Ausfall des Servers **28**
Ausgleichen des Festplattenzugriffs **101**
Ausstehende Festplattenanforderungen **101**
Authentifizierung **13, 48, 84**

B

Beanspruchen von Pfaden **89**
Beanspruchungsregeln **89**
Befehle
  esxcli corestorage claimrule **114**
  resxtop **113**
  vicfg-iscsi **113**
  vicfg-mpath **113**
  vmkping **114**
Beiderseitiges CHAP **48**
Bevorzugter Pfad **90**

C

CHAP
  Beiderseitig **48**
  deaktivieren **52**
  Für Erkennungsziele **50**
  Für iSCSI-Initiatoren **49**
  Für statische Ziele **50**
  Unidirektional **48**
CHAP-Authentifizierung **13, 48, 84**
CHAP-Authentifizierungsmethoden **48**
Checkliste **111**

D

Dateibasierte Lösung (VMFS) **105**
Daten-Digests **14**
Datenspeicher
  Aktualisieren **85**
  Anzeigen **83**
  Erstellen auf iSCSI-Speicher **56**
  mounten **106**
  Pfade **90**
  Überprüfen von Eigenschaften **84**
  Unmounten **106**
  Verwalten von Duplizierten **105**
Datenspeicherkopien, mounten **105**
Datenträger-Zeitüberschreitungswert **94**
Deaktivieren von Pfaden **93**
Dell PowerVault MD3000i-Speichersysteme **67**
Diagnosepartitionen, gemeinsam nutzen **94**
Disk.MaxLUN **87**
Disk.SchedNumReqOutstanding **101**
Disk.SupportSparseLUN **87**
Drittanbieter-Sicherungspaket **104**
Dump-Partitionen, gemeinsam nutzen **94**
dynamische Erkennung, konfigurieren **46**
Dynamische Erkennungsadressen **46**

E

E/A-Verzögerung **26, 32**
EMC CLARiiON **60**
EMC Symmetrix, Pseudo-LUNs **61**
EqualLogic, Speichersysteme **66**
Erkennung
  Adresse **46**
  Dynamisch **46**
  statisch **47**
Erneut prüfen
  LUN-Anzeige **29**
  LUN-Erstellung **84–86**
  LUN-Maskierung **84**

Pfadmaskierung **85, 86**
wenn Pfad nicht verfügbar ist **85, 86**
erweiterte Einstellungen
Disk.MaxLUN **87**
Disk.SchedNumReqOutstanding **101**
Disk.SupportSparseLUN **87**
ESX/ESXi-Hosts
gemeinsame Nutzung eines VMFS **17**
Und iSCSI-SAN **79**
esxcli corestorage (Befehl), Optionen **125**
esxcli corestorage claimrule-Befehl **114**
ESXi, Konfigurieren für Netz-Dump **78**
EUI **10**
EVA (HP StorageWorks) **63**

F

Failover
E/A-Verzögerung **26**
Transparent **13**
Failover-Pfade, Status **90**
Fehlerbehebung
Ändern der iSCSI-Startparameter **77**
Netzwerkverbindung unterbrochen **76**
Fest, Pfadrichtlinie, Pfad-Thrashing **100**
Festplatten-Arrays
aktiv/aktiv **32, 91**
aktiv/passiv **32, 91, 100**
Festplattenfreigaben **20**
Festplattenzugriff, ausgleichen **101**
FilerView **64**

G

Gemeinsame Nutzung eines VMFS durch mehrere Server **17**
Gemeinsame Nutzung von Diagnosepartitionen **94**

H

Hardware-iSCSI, und Failover **24**
Hardware-iSCSI-Adapter
Abhängig **11**
unabhängig **11**
Hardware-iSCSI-Initiatoren
Ändern des iSCSI-Namens **34**
anzeigen **34**
Einrichten von Benennungsparametern **34**
Einrichten von Erkennungsadressen **46**
installieren **34**
konfigurieren **33**
Hardwarebeschleunigung
Anforderungen **108**
deaktivieren **109**
Grundlegende Informationen **108**
Löschen von Beanspruchungsregeln **125**
Status **109**
Vorteile **108**
Hardwarebeschleunigungs-Plug-Ins **115**
Header-Digests **14**
Hoch, Qualitätsstufe für Speicher **27**
Hosttyp **60**
HP LeftHand P4000 VSA **67**
HP StorageWorks
EVA **63**
MSA **62**

I

iBFT **72**
iBFT-iSCSI-Start
Ändern der Startsequenz **74**
Einrichten von ESXi **73**
Einschränkungen **73**
Fehlerbehebung **76**
Installieren eines ESXi-Hosts **75**
Optimale Vorgehensweisen für Netzwerke **75**
Starten eines ESXi-Hosts **75**
IP-Adresse **10**
IQN **10**
iSCSI, Mit mehreren Netzwerkkarten **40**
iSCSI-Adapter
Grundlegende Informationen **31**
Hardware **11**
Software **11**
iSCSI-Alias **10**
iSCSI-HBA, Alias **34**
iSCSI-Initiatoren
Anzeigen im vSphere-Client **79**
CHAP konfigurieren **49**
Einrichten von CHAP-Parametern **48**
Erweiterte Parameter **52**
Hardware **33**
Konfigurieren erweiterter Parameter **53**
iSCSI-Namen, Konventionen **10**
iSCSI-Netzwerk, Erstellen eines VMkernel-Ports **40**
iSCSI-Ports **10**
iSCSI-SAN
Boot **69**
Konzepte **9**
iSCSI-Sitzungen
Anzeigen **54**
Duplizieren **55**
entfernen **56**
Hinzufügen für ein Ziel **55**
verwalten **54**
iSCSI-Speicher, hinzufügen **56**
iSCSI-Speichersysteme, Arbeiten mit ESX/ESXi **59**
iSCSI-Start, iBFT **72**

iSCSI-Start-Firmware-Tabelle, *, siehe* iBFT
iSCSI-Startparameter, konfigurieren **74**

J
Jumbo-Frames
  Aktivieren für abhängige Hardware-iSCSI **45**
  Aktivieren für Software-iSCSI **45**
  Verwenden mit iSCSI **45**

K
konfigurieren
  dynamische Erkennung **46**
  iSCSI-Speicher **56**
  statische Erkennung **47**

L
Lastausgleich, manuell **93**
LeftHand Networks SAN/iQ-Speichersysteme **66**
Leistung
  Netzwerk **97**
  optimieren **95**
  Probleme **99**
  SCSI-Reservierungen **17**
  Speichersystem **96**
  Überprüfen von Ethernet-Switch-Statistiken **99**
Linux-Clusterhosttyp **60**
Linux-Hosttyp **60**
LUN-Erkennung, VMkernel **29**
LUN-Wahl
  Adaptives Modell **20**
  Vorhersagemodell **19**
LUNs
  Ändern der Anzahl an LUNs, nach denen gesucht wird **87**
  Änderungen vornehmen und erneut prüfen **85**
  anzeigen und erneutes Prüfen **29**
  ein VMFS-Volume pro LUN **32**
  Entscheidungen **18**
  Erstellen und erneut prüfen **84, 86**
  Festlegen einer Multipathing-Richtlinie **91**
  Maskierung **119**
  Multipathing-Richtlinie **91**
  Sparse **87**
  Zuordnungen **32**
LUNs, die nicht angezeigt werden, Speicherprozessoranzeige **84**

M
Manueller Lastausgleich **93**
Maskierung von LUNs **119**
Mehrschichtige Anwendungen **104**
Mittel, Qualitätsstufe für Speicher **27**
Mounten von VMFS-Datenspeichern **105**
MPPs
  Anzeigen **116**
  Siehe auch Multipathing-Plug-Ins
MSA (HP StorageWorks) **62**
MTU **45**
Multipathing
  aktive Pfade **90**
  Aktivieren für Software-iSCSI **43**
  Anzeigen des aktuellen Status **90**
  beschädigte Pfade **90**
  deaktivierte Pfade **90**
  Standby-Pfade **90**
Multipathing-Beanspruchungsregeln
  hinzufügen **117**
  löschen **119**
Multipathing-Plug-Ins, Beanspruchen von Pfaden **89**
Multipathing-Richtlinie **91**
Multipathing-Status **90**

N
NAA **10**
Natives Multipathing-Plug-In **22, 23**
NetApp
  Bereitstellen von Speicher über die CLI **65**
  Bereitstellen von Speicher über FilerView **64**
NetApp-Speichersystem **63**
Netz-Dump
  Konfigurieren von ESXi **78**
  Konfigurieren von vMA **78**
Netzwerk, konfigurieren **33**
Netzwerkadapter, Konfigurieren für den iBFT-iSCSI-Start **74**
Netzwerkkarten, Zuordnen zu Ports **41**
Netzwerkleistung **97**
Netzwerkverbindung unterbrochen, Fehlerbehebung **76**
Netzwerkvirtualisierung **8**
NFS-Datenspeicher, Unmounten **106**
Niedrig, Qualitätsstufe für Speicher **27**
NMP
  Beanspruchen von Pfaden **89**
  E/A-Fluss **24**
  Siehe auch Natives Multipathing-Plug-In
Notfallwiederherstellung **15**

P
Passive Festplatten-Arrays, Pfad-Thrashing **100**
Pfad-Failover
  Array-basiert **26**
  Hostbasiert **24**
Pfad-Thrashing, Beheben **101**
Pfadausfall, erneutes Prüfen **85, 86**

Pfadauswahl-Plug-Ins **24**
Pfade
  bevorzugt **90**
  deaktivieren **93**
  Maskierung **119**
  Maskierung aufheben **120**
Pfadrichtlinien
  Ändern des Standardeinstellungen **92**
  Fest **24, 26, 91**
  Round Robin **24, 91**
  Zuletzt verwendet **24, 91**
Pfadverwaltung **21, 93**
Plug-Ins
  Hardwarebeschleunigung **115**
  Multipathing **115**
Port-Bindung, Beispiele **44**
Port-Bindung entfernen **44**
Portumleitung **26**
Priorisieren virtueller Maschinen **20**
Probleme
  Anzeige **84**
  Leistung **99**
Prüfen, Anzahl ändern **87**
PSA, *, siehe* Pluggable Storage Architecture
PSPs, *, siehe* Pfadauswahl-Plug-Ins

R

Reservierungen, Reduzieren von SCSI-Reservierungen **102**
resxtop-Befehl **113**
Round Robin, Pfadrichtlinie **24, 91**

S

SAN
  Besonderheiten **16**
  Fehlerbehebung **95**
  Server-Failover **28**
  Sicherung, Überlegungen **103**
  Vorteile **14**
  zugreifen **21**
SAN (Storage Area Network) **7**
SAN-Beschränkungen, beim Arbeiten mit ESX/ESXi **32**
SAN-Speicherleistung optimieren **95**
SAN-Verwaltungssoftware **16**
SATPs
  Anzeigen **117**
  Regeln hinzufügen **120**
  Siehe auch Plug-Ins für Speicher-Array-Typen
Schulungssupport **5**
SCSI-Controller **8**
SCSI-Reservierungen reduzieren **102**
Server-Failover **28**
Serverausfall **28**
Serverleistung **96**
Sicherungen
  Drittanbieter-Sicherungspaket **104**
  Überlegungen **103**
Snapshot-Software **103**
Software-iSCSI
  Netzwerk **39**
  und Failover **24**
Software-iSCSI-Adapter, Warteschlangentiefe **102**
Software-iSCSI-Initiatoren
  aktivieren **37**
  Einrichten von Erkennungsadressen **46**
  konfigurieren **37**
Software-iSCSI-Start, Ändern von Einstellungen **76**
Sparse-LUN, Unterstützung **87**
Speicher-Array-Typ, Plug-Ins **23**
Speicheradapter
  Anzeigen im vSphere-Client **79, 80**
  Kopieren von Namen in die Zwischenablage. **80**
Speicherfilter
  deaktivieren **87**
  Erneute Hostprüfung **88**
  für denselben Host und dieselben Transports **88**
  RDM **88**
  VMFS **88**
Speichergeräte
  Anzeigen **117**
  Anzeigen von Daten **80**
  benennen **81**
  Bezeichner **83**
  Für Hosts verfügbar **82**
  Hardwarebeschleunigungs-Status **122**
  Pfade **91**
  Zugriff über Adapter **82**
Speicherort von virtuellen Maschinen **27**
Speicherprozessoranzeige, LUN wird nicht angezeigt **84**
Speichersysteme
  Dell PowerVault MD3000i **67**
  EMC CLARiiON **60**
  EMC Symmetrix **61**
  EqualLogic **66**
  HP StorageWorks **62**
  LeftHand Networks SAN/iQ **66**
  Leistung **96**
  NetApp **63**
  Typen **13**
Speichervirtualisierung **8**

Starten von einem iSCSI-SAN
  Hardware-iSCSI **71**
  iBFT **72**
  Konfigurieren der iSCSI-Einstellungen **72**
  Konfigurieren von HBAs **71**
  Richtlinien **70**
  Software-iSCSI **72**
  Vorbereiten des SAN **70**
statische Erkennung, konfigurieren **47**
Statische Erkennungsadressen **46**
Sternchen neben dem Pfad **90**
Suchen nach Informationen **16**

T

Technischer Support **5**
Testen, Speichersysteme **59**
TimeoutValue-Parameter **32**

U

Unidirektionales CHAP **48**
Updates von Metadaten **18**

V

VAAI-Beanspruchungsregeln
  Definieren **124**
  löschen **125**
  VAAI-Filter **124**
  VAAI-Plug-In **124**
VAAI-Filter, Anzeigen **122**
VAAI-Plug-Ins
  Anzeigen **122**
  Auflisten für Geräte **123**
Verwaltungsanwendungen von Drittanbietern **16**
vicfg-iscsi-Befehl **113**
vicfg-module **102**
vicfg-mpath-Befehl **113**
Virtualisierung **7**
virtuelle Maschinen
  Ausgleichen des Festplattenzugriffs **101**
  E/A-Verzögerung **26**
  priorisieren **20**
  Speicherort **27**
  Zugriff auf das SAN **21**
vMA, Erfassen des Netz-Dumps **77**
vMA, Konfigurieren für Netz-Dump **78**
VMFS
  ein VMFS-Volume pro LUN **32**
  Gemeinsame Verwendung auf ESX/ESXi-Hosts **17**
  Volume-Neusignierung **105**
VMFS-Datenspeicher
  Ändern von Signaturen **107**
  Neusignierung von Kopien **107**
  Unmounten **106**
VMFS-Volume-Neusignierung **105**
VMkernel, LUN-Erkennung **29**
VMkernel-Ports **41**
VMkernel-Schnittstelle, für Jumbo-Frames aktiviert **46**
vmkping-Befehl **114**
vMotion **14, 15, 32, 60**
VMware DRS, Mit VMotion **32**
VMware HA **14, 28, 60**
VMware NMP
  E/A-Fluss **24**
  Siehe auch Natives Multipathing-Plug-In
VMware PSPs, *, siehe* Pfadauswahl-Plug-Ins
VMware SATPs, *, siehe* Plug-Ins für Speicher-Array-Typen
Volume-Neusignierung **105, 107**
Vorhersagemodell **19**
vSphere-CLI **43**
vSphere-Client **113**
vSwitch, für Jumbo-Frames aktiviert **45**

W

Warteschlangentiefe **32, 102**
Wartung **15**

Z

Zeitüberschreitung für das Gastbetriebssystem **94**
Ziele **12**
Ziele im Vergleich zu LUNs **12**
Zugriffssteuerung **13**
Zuletzt verwendet, Pfadrichtlinie, Pfad-Thrashing **100**
Zuordnungen, LUN **32**